# NCF

# Webmasters

# Handbook

Edition 1

# Table of Contents

| | |
|---|---|
| Date prepared: | 23 March 2001 |
| Prepared By: | Scott D Wilson EOC (ret)<br>wilsonsd@nitc.navfac.navy.mil<br>805.982.3601 |

## Chapter 1

# Introduction

Welcome to the first edition of the NCF Webmasters Handbook. This handbook is a desktop reference for all NCF Webmasters, not just a rewrite of available books and instructions.

This handbook was created for the First Annual NCF Webmaster Conference. The content covers problem areas that may confuse the average user as well as topics that may benefit the NCF Webmasters. The handbook provides the NCF Webmaster with all the necessary resources to administer and manage their Command Web sites within the constraints of DoD, NAVFAC, and NCF policies.

### Objectives

This handbook has five objectives:

- Provide all applicable instructions for managing publicly accessible Web sites as well as policy guidelines for the Web site management on the NCF Corporate Intranet.
- Configure computer workstations for use with Microsoft Peer Web Server and accomplish specific tasks using Microsoft FrontPage 2000.
- Illustrate Web-based applications available to all Webmasters on both the NCF Corporate Intranet and NCF Internet domains.
- Standardize all Web sites hosted on the NCF Corporate Intranet.
- Troubleshoot errors in FrontPage.

### How this manual is organized

The handbook covers all the areas that I felt are most important for the Unit Webmasters to effectively develop and mange their respective Web sites. The manual is broken into 8 separate chapters.

**Chapter 1** - Introduces the handbook.

**Chapter 2** - References all applicable instructions governing Web site administration for publicly accessible Web sites and policy guidelines enforced on the NCF Corporate Intranet.

**Chapter 3** - Explains the difference of the individual Web sites and their intended purpose.

**Chapter 4** - Illustrates how to configure a workstation for use with Peer Web Server and defines PKI server certificates and how to import them.

**Chapter 5** - Demonstrates how to accomplish many of the tasks that are required to effectively maintain Command Web sites.

**Chapter 6** - Identifies Web-based applications available on the NCF Corporate Intranet.

**Chapter 7** - Identifies the importance of standardizing information dissemination on the NCF Corporate Intranet.

**Chapter 8** –Provides a record of the discussions and concerns expressed during the conference.

# Chapter 2

## Policies / Instructions

1. **DoD policy memorandum 11/98, Web Site Administration Policy and Procedures**
   (http://www.defenselink.mil/admin/dod_Web_policy_12071998.pdf)

   DoD policy memorandum provides the DoD policy, assigns responsibility, and describes the procedures for establishing, operating and maintaining DoD unclassified Web sites.

2. **SECNAV Instruction 5720.47, Department of the Navy Policy for Content of Publicly Accessible World Wide Web Sites**
   (http://www.chinfo.navy.mil/navpalib/internet/5720-47.pdf)

   This instruction implements item (1) within the Department of the Navy (DoN) and provides additional policies and procedures governing the content of Department of the Navy publicly accessible World Wide Web (WWW) sites.

3. **COMSECONDNCB/COMTHIRDNCB Instruction 2000.1, Internet Policy**
   (http://www.seabee.navy.mil/help/instruct/2000.1.pdf)

   This instruction establishes COMSECONDNCB/ COMTHIRDNCB policy on Internet access and use of Government Information Systems.

4. **COMSECONDNCB/COMTHIRDNCB Notice 2000, Web Site Administration**
   (http://navfacilitator.navfac.navy.mil/ncf/docs/notice/Joint 2000 notice.pdf)

   This notice provides guidance and assigns responsibility for adminisistering and maintaining an unclassified, publicly accessible Web information service within the NCF.

5. **COMSECONDNCB/COMTHIRDNCB Instruction 5780.1, NCF Internet / Intranet Policy Guidelines**

   This instruction provides policy guidance for all applicable Web sites designed, developed, procured, or managed on the NCF Domain servers. Instruction is not yet available for release.

6. **Assistant Secretary of Defense, Policy Guidance for use of Mobile Code Technologies in Department of Defense (DoD) Information Systems** (https://infosec.navy.mil/pub/docs/navy/Mobile_Code_Memo_11-7-00.pdf)

   The policy memorandum categorizes mobile code technologies and defines their use within DoD Information Systems based on their potential to process, transmit, store, or display DoD information. This includes commercial off-the-shelf (COTS) products and electronic commerce applications used but not necessarily owned by the government.

7. **Department of the Navy NIPRNET Firewall Policy (Shore and Afloat)** (https://infosec.navy.mil/pub/docs/navy/FLEET/FLEETFWPOLICY.pdf)

   The policy is divided into the three Open Source Interconnection (OSI) layers that are normally filtered by fleet firewalls; the Network Layer (Layer 3), the Transport Layer (Layer 4), and the Application Layer (Layer 7). Each of the three layers is broken out in its own table; the Network Layer table sorted by protocol number, the Transport Layer table by TCP/UDP port number, and the Application Layer table in alphabetical order of the applications/services.

8. **NAVFAC Intranet StyleGuide** (http://navfacilitator.navfac.navy.mil/about/stylegui.htm)

   The NAVFAC Intranet Style Guide provides basic guidance to authors and editors for preparing corporate intranet pages for consistent and readable presentation of information. It is not intended to be a complete style guide for composing web pages.
   The emphasis in this guide is on simplicity. Note that intranet sites differ from Internet sites in that there is a heavier emphasis on supporting workflow processes, documentation management, and work collaboration, with more functionality and less "glitz."

9. **36 CFR Part 1194, December 21, 2000, Architectural and Transportation Compliance Board. (Final Rule)** (http://www.access.gpo.gov/nara/cfr/index.html)

   **Section 1194.22 Web-based Intranet and Internet Information and Applications**. Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

10. **36 CFR Part 1194, March 31, 2000, Architectural and Transportation Compliance Board. (Proposed Rule)** (http://www.access.gpo.gov/nara/cfr/index.html)

    Same as above.

This page left intentionally blank

# Chapter 3

## Web Site Information Management

This page left intentionally blank

## 1. Overview

It’s important to explain the significance and purpose of each type of Web site.

Note: Web sites should be updated and approved at the local Command before being published to the domain server. Only under extenuating circumstances and with the approval of the NCF Webmaster shall data be changed, updated, or otherwise managed online while logged into the NCF Domain Server. DoD strictly prohibits managing publicly accessible Web sites online. These Web sites have specific requirements for release of information to the public.

## 2. Publicly Accessible Web Sites

Publicly accessible Web sites are designed to inform the general public, whom should therefore be considered the target audience. The NCF Internet Web site template provides ease of navigation through all NCF Web sites and maintains a consistent look and feel amongst all NCF Units. One primary goal of the initial Web site template is to convey to the public a sense that there is only one NCF.

Information generated for publicly accessible Web sites should be handled as news releases and, therefore, has to be cleared for public release. Approval may usually be granted at the Unit level. Items identified in Chapter 2, Item 1 are strictly prohibited. Elevate the approval process up the Chain of Command for content not prohibited but may be deemed inappropriate.

The Unit’s Public Affairs Officer is responsible for reviewing all content before releasing it to the general public. FrontPage 2000 can provide a listing of all new or changed documents for their review prior to releasing the information to the Seabee Internet Web Server.

The publicly accessible Web sites are informational in nature and should not be considered a tool in which to conduct business. There are other means in place to satisfy this requirement (e.g. NCF Corporate Intranet and F&F Web sites).

The intent of the publicly accessible Web sites is to provide general information about the U.S. Navy Seabees, their individual missions, and how they integrate with the U.S. Navy and American Forces abroad.

## 3. Friends and Family Web Sites

Friends and Family Web sites (referred to as F&F Web sites) are provided for a specifically targeted audience at the request of the Unit Commanders. These Web sites are classified as private and are restricted to authorized users. It is the responsibility of the individual Commands to grant access to these Web sites and not the NCF Webmaster. The F&F Web sites have been created for all deployable and reserve Units, as well as those who have requested one with sufficient justification warranting it.

The intent of the F&F Web sites is to post data that doesn't qualify as classified but violates the requirements of DoD policy. Examples of information posted to the F&F Web sites may include but is not limited to PODs / POWs, names with pictures, detailed contact information, or anything the Command deems necessary for its target audience

The F&F Web sites are not regulated as to the format or information content with the exception of classified information. The NCF Webmaster has a responsibility to routinely review the Web sites, policing for inappropriate or restricted information.

## 4. Intranet Web sites

The NCF Corporate Intranet is designated For Official Use Only (FOUO). These sites will be discussed in greater detail in Chapter 7. This section briefly explains the benefits of the Intranet, which is intended to share information to a broader Navy audience and to provide a data store for people and Units.

The NCF and NAVFAC Corporate Intranets provide a vast data pool of information relevant to how well we conduct our business day-to-day. Establishing information standards and how and where it's posted is extremely important to its success. The goal is to post information from site to site in the same basic manner to minimize browsing time, hence providing a more suitable resource for everyone.

For more specific information on the NCF Corporate Intranet please see Chapter 7.

# Chapter 4

## Workstation Configuration

This page left intentionally blank

## 1. Overview

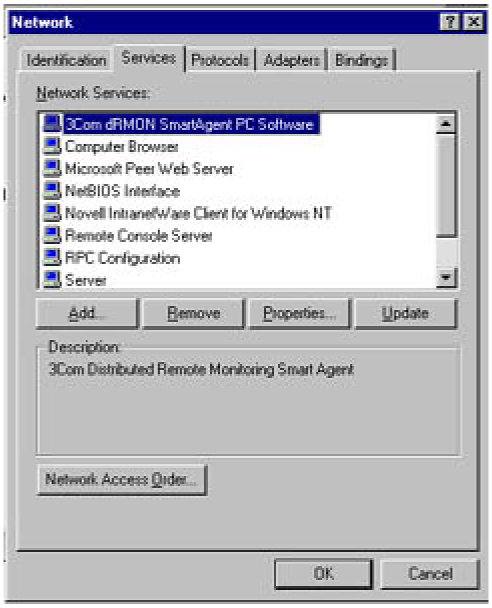
The first step to effectively manage a web site locally is to correctly configure the workstation. The standard Operating System in the NCF is Microsoft Windows NT 4.0; therefore Microsoft Peer Web Services should be installed first.

Microsoft Peer Web server is a personal Web server that has been optimized to run on Windows NT Workstation version 4.0. With Peer Web Services, you can create a personal Internet server, which is ideal for development, testing, and peer-to-peer publishing.

For those Units that are administering their web sites on Microsoft Windows 95 /98, FrontPage 2000 will by default install FrontPage Personal Web Server which requires no additional configuration.

## 2. Installing Microsoft Peer Web Server

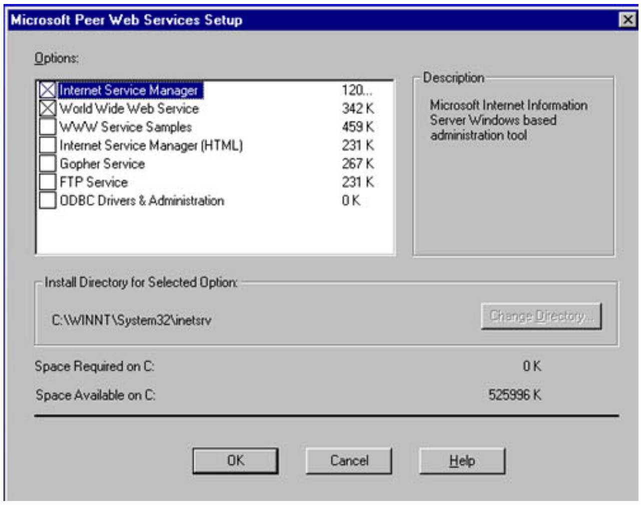
1. Click the Windows **Start** button, point to **Settings**, and click **Control Panel**.
2. Double-click the **Network** icon.
3. Click the **Services** tab, and then click **Add**.
4. In the first **Microsoft Peer Web Services Setup** dialog box, click **OK**.



Network Services:

- 3Com dRMON SmartAgent PC Software
- Computer Browser
- Microsoft Peer Web Server
- NetBIOS Interface
- Novell IntranetWare Client for Windows NT
- Remote Console Server
- RPC Configuration
- Server

Description:
3Com Distributed Remote Monitoring Smart Agent



Options:

| | |
|---|---|
| ☒ Internet Service Manager | 120... |
| ☒ World Wide Web Service | 342 K |
| □ WWW Service Samples | 459 K |
| □ Internet Service Manager (HTML) | 231 K |
| □ Gopher Service | 267 K |
| □ FTP Service | 231 K |
| □ ODBC Drivers & Administration | 0 K |

Description
Microsoft Internet Information Server Windows based administration tool

Install Directory for Selected Option:
C:\WINNT\System32\inetsrv

Space Required on C: 0 K
Space Available on C: 525996 K

5. In the second **Microsoft Peer Web Services Setup** dialog box, select the top two boxes (Internet Service Manager and World Wide Service), uncheck all remaining, then click **OK**.

6. Click **OK** to create the **<system root>\system32\inetserv** folder.

7. In the **Publishing Directories** dialog box, specify the location you want to create the **inetpub\wwwroot** folder, or accept the default directory and then click **OK**.

Note: If you are not presented with step 7, then the installation did not complete correctly even though the dialog box indicates it did. To verify the if the local web server is operating correctly,

1. Select **Start**, **Programs**, **Microsoft Peer Web Services (Common)**, **Internet Service Manager**.
2. In the open window what should appear is the **local host name** (your computer name), **www** service and should indicate it's **running**.
3. If the window is blank then proceed to the next section (Correcting the installation).

### 3. To correct the installation

1. Select **Start**, **Programs**, **Microsoft Peer Web Services (Common)**, **Peer Web Services Setup.**

2. In the first **Microsoft Peer Web Services Setup** dialog box, select **Reinstall**.

3. The installation will begin.

4. A dialog box will appear indication that a file already exists and gives the options to **Cancel**, **Retry** or **Ignore**. Select **Ignore** as many times as the dialog box appears.

5. Click **OK** when the dialog box appears indicating the Installation Completed Correctly.

6. Then select **Start**, **Programs**, **Microsoft Peer Web Services (Common)**, **Peer Web Services Setup.**

7. In the first **Microsoft Peer Web Services Setup** dialog box, select **Remove all**.

8. Repeat steps 1 through 7 above in the section Installing Microsoft Peer Web Server.

## 4. Importing the PKI Server Certificates

This section requires that the end user is actively using Microsoft Internet Explorer 5.0 or above.

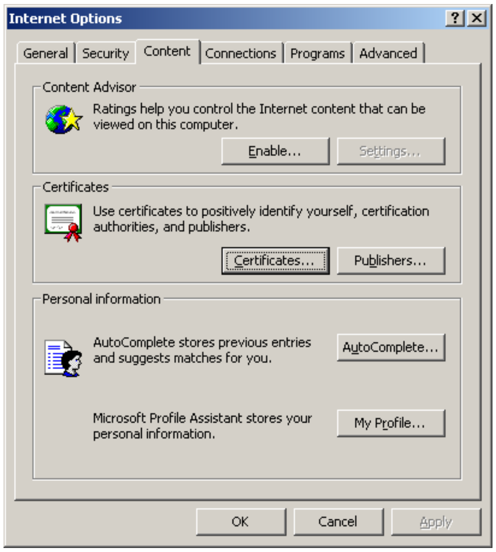
1. Download the **PKI Server Certificates** from http://www.seabee.navy.mil/help/SSL/ssl.htm

2. Minimize the Web Browser to the Task Bar.

3. Unzip the **DODcert.zip** to a location that is easy to find.

   Two files will be extracted to the desktop: DoDcert.cer and MedCA1.cer

4. Maximize the Web Browser from the Task Bar.



Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

5. From the top line menu, select **Tools**, **Internet Options.**

6. Click the **Content** tab, **Certificates**.

7. Select the **Trusted Root Certification Authorities** tab on the top, **Import.**

8. Click **Next** on the Welcome to the Certificate Import Wizard dialog box.

9. Click **Browse** and navigate to the location the **DODcert.zip** was extracted.

10. Click the down arrow on the **File of Type** and select **X.509 Certificates (*.cer, *.crt)**.

11. Select **DODcert.cer** and click **Open**.

12. Click **Next** and except the default settings on the remaining dialog boxes and then **Finish** on the last one.

13. When prompted to accept the certificate, click **OK**.

14. From the **Content** tab, **Certificates** dialog box.

15. Select the **Intermediate Certification Authorities** tab, **Import.**

16. Click **Next** on the Welcome to the Certificate Import Wizard dialog box.

17. Click **Browse** and navigate to the location the file.zip was extracted.

18. Click the down arrow on the **File of Type** and select **X.509 Certificates (*.cer, *.crt)**.

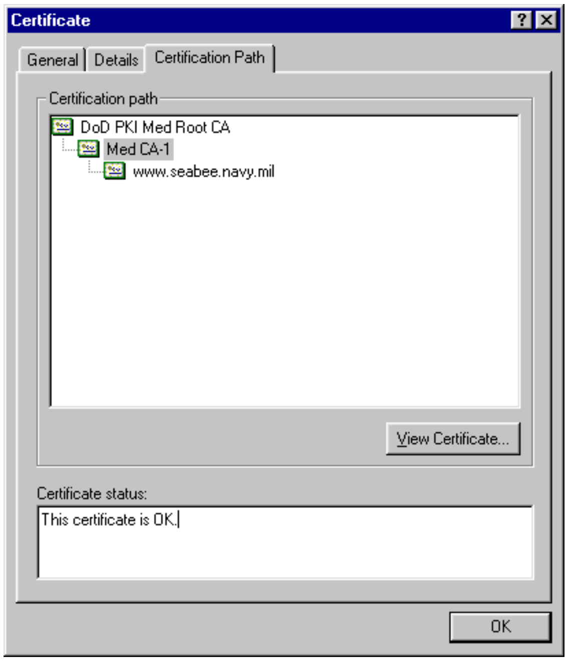
19. Select **medCA1.cer** and click **Open**.

20. Click **Next** and except the default settings on the remaining dialog boxes and then **Finish** on the last one.

21. When prompted to accept the certificate, click **OK**.

22. Browse to https://www.seabee.navy.mil/ and insure the **yellow lock** appears in the bottom right corner [IE] or bottom left corner [Netscape] of the web browser window.

23. Double clicking the lock and selecting the **Certification Path** tab from the **Certificate** dialog box should indicate a path as illustrated to the right.



Certification path

- DoD PKI Med Root CA
  - Med CA-1
    - www.seabee.navy.mil

Certificate status:

This certificate is OK.

# Chapter 5

## Routine tasks in FrontPage 2000

This page left intentionally blank

## 1. Overview

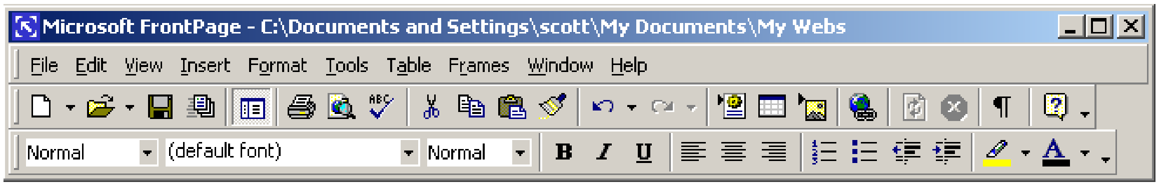
To effectively capture an entire audience, Webmasters should ensure cross compliance with all web browsers. Creating web pages is not a difficult task, but ensuring everybody can see them is considerably more time consuming and task oriented.

Before publishing a web site into production, a series of things should be considered first. Validating the hyperlinks, ensuring no orphans exist, checking cross compliance of the web with other browsers (Netscape and I.E.). **Note:** Netscape web browsers are not as forgiving as I.E. Missing or erroneous tags, ActiveX components and other inserted FrontPage features will render pages inaccessible. Many of the tasks are identified in this section of the Handbook, but others have to be completed with additional third party software (e.g. Netscape Navigator)

The operations explained in this chapter assume the user has FrontPage 2000 open and in an active window.

Navigating in FrontPage is typical of most all Microsoft products. The menus appear basically the same with exception to the items that are unique to FrontPage 2000.

The main menu bar is a useful tool providing quick access the basic features used to create web pages.


Microsoft FrontPage - C:\Documents and Settings\scott\My Documents\My Webs
File Edit View Insert Format Tools Table Frames Window Help
Normal
(default font)
Normal
B
I
U

Buttons appearing from the top left:

- Create a New Page
- Open File
- Save As
- Publish Web
- Show Folder List
- Print Page
- Preview in a Browser
- Check Spelling
- Cut
- Copy
- Paste

Buttons appearing from the bottom left:

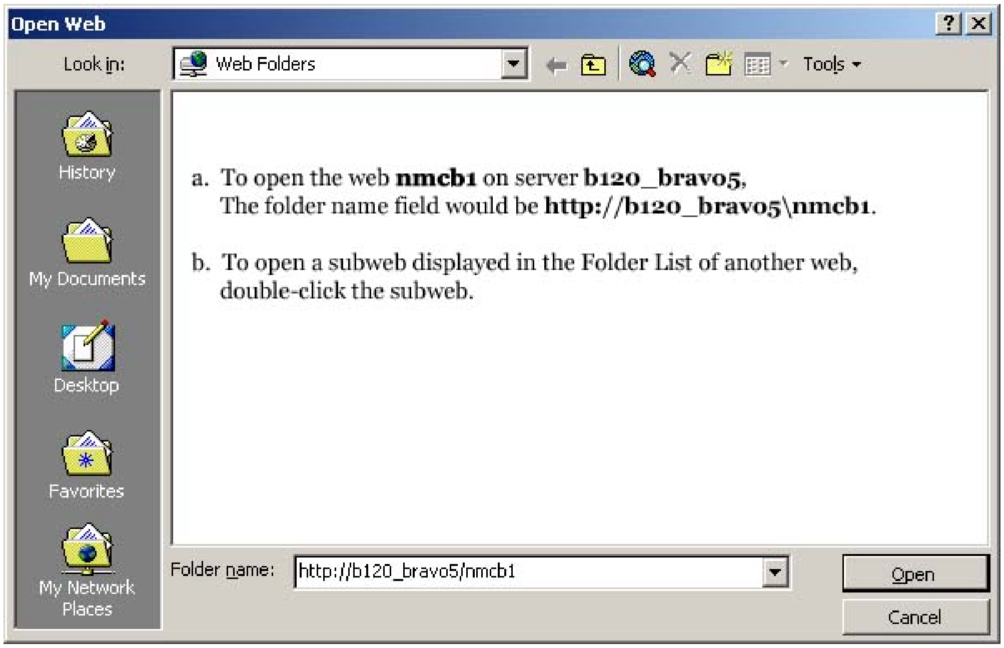
- Select Heading
- Select Font type
- Select Font size
- Bold
- Italics
- Underline
- Align Left
- Align Center
- Align Right
- Insert Numbered List
- Insert Bulleted List

- Format Painter
- Undo
- Redo
- Insert FrontPage Component
- Insert Table
- Insert Image
- Insert Hyperlink
- Refresh Page
- Stop
- Show All Tags
- Help
- Decrease Indent
- Increase Indent
- Highlight Color
- Font Color

## 2. Opening a Web

a. From the top line menu select **File**, **Open Web**.

b. To open a web on a server, in the **Folder Name** box, type the URL to that web, and then click **Open.** For example:



a. To open the web **nmcb1** on server **b120_bravo5**,
The folder name field would be **http://b120_bravo5\nmcb1**.

b. To open a subweb displayed in the Folder List of another web,
double-click the subweb.

Folder name: http://b120_bravo5/nmcb1

**Note:**

- To open a web that you've opened recently, in the **Open Web** dialog box, click the drop-down arrow at the right of the **Folder Name** box, click the web you want, and then click **Open**. Or, if you aren't in the **Open Web** dialog box, point to **Recent Webs** on the **File** menu, and then click the desired web.

- To open the last web you worked on automatically each time you start FrontPage, click **Options** on the **Tools** menu, and then select the **Open last web automatically when FrontPage starts** check box.

- In the **Open Web** dialog box, click an icon on the left (such as History, Favorites, or Web Folders) to open a web in one of those locations.

- If you already have a web open, each subsequent web opens in a new FrontPage window.

## 3. Creating a New Folder / Page

### a. New Folders

1) Right-click in the Folder List, and then click **New Folder** on the shortcut menu.

2) Type the name of the new folder, and then press **ENTER**.

### b. New Pages

1) In the Folder List, right-click the folder in which you want to create the new page, and then click **New Page** on the shortcut menu. Type the name of the new page, and then press **ENTER**.

   **Note:** If you right-click the background of the Folder List without selecting a folder, the new page will be created in your root web.

2) On the File menu, point to **New**, and then click **Page**.

## 4. Saving a Page

### a. Save As

1) If the page was opened from a location outside the current web or a page is used as a template, click **Save As** on the **File** menu. Navigate to the folder or location in the web where you want to save the page. Type the file name of the page in the File name box. Change the page title by clicking the **Change** button and entering the new page title in the **Page Title** box. Click Save.

### b. Save as a Template

1) Using the same method as mentioned above, click the drop-down arrow at the right of the **Save as Type** box and change to **FrontPage Template (*.tem)**. Click Save.

   > **Note**: FrontPage will save the page to the Office\Template folder. To use the page select it from **File** menu, **New Page** and click on the new page template.

## 5. Importing into FrontPage

### a. Importing Files

1) To import files, click **Add File**.

2) In the **Add File to Import List** dialog box, point to the folder where the files you want to import are stored.

3) Select the files, and click **Open**.

### b. Import a Folder

1) To import a folder, click **Add Folder**, and then in the **Browse for Folder** dialog box, locate and select the folder, and then click **OK**.

### c. Import from a Web

1) To import a file or folder from a Web site, click **From Web**, and then respond to the Import Web wizard. Enter the complete URL in the **Location** box.

   **Note**: To add additional files from other folders, more folders, or files from other Web sites to the Import list, repeat this procedure listed above.

## 6. Publishing FrontPage Webs

Publishing webs using FrontPage is equivalent to copying the contents of the existing web to an alternate location. The user has a series of options when publishing FrontPage webs.

a. Publish only the files that have changed. FrontPage compares the files on your local web to the files on the Web server, and only those files that are newer than those on the Web server are published. However, files that have been marked *Don't Publish* will not be published.

1) **Mark a page *Don’t Publish***

   If you have not finished editing a page but you want to publish your Web site, you can prevent the page from being published by marking it *Don't Publish*.

   Certain files should not be published again after you first publish your web. For example, you create a web with a guestbook, and then publish the web. Later, you update your web pages — if you publish all of your files, including the file that records guestbook information, you will save a blank guestbook over the existing one, losing all the information. Other examples include pages with a hit counter; discussion webs; and catalogs (if you are running Index Server).

   i. Select one or more files, right-click them, click **Properties** on the shortcut menu, and then click the **Workgroup** tab.

   ii. Do one of the following:

      1. To prevent a file from being published, select the **Exclude this file when publishing the rest of the web** check box.
      2. To mark a file for publishing, clear the **Exclude this file when publishing the rest of the web** check box.

b. Publish all files, except those that have been marked *Don't Publish*. The files from the local web will overwrite all files on the destination Web server, even if the files on the Web server are newer.

c. Publish subwebs, if the current web has subwebs. All files and folders in subwebs will be recursively published in addition to those in the current web.

d. Publish the web using a secure (SSL) connection. For example, use this feature if your Web server uses the HTTPS protocol to authenticate its users.

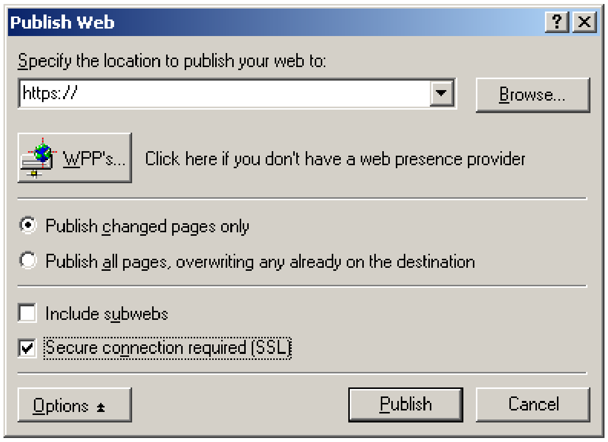
   1) On the **File** menu, click **Publish Web**.

   2) Click **Options** to expand the list of options.

   3) Specify whether you want to publish only pages that have changed, or all pages.

4) To publish subwebs, select the **Include subwebs** check box.

5) To publish using a secure connection, select the **Secure connection required (SSL)** check box. (Use this selection when publishing to the NCF domain servers).



Publish Web

Specify the location to publish your web to:

https://

Click here if you don't have a web presence provider

● Publish changed pages only

○ Publish all pages, overwriting any already on the destination

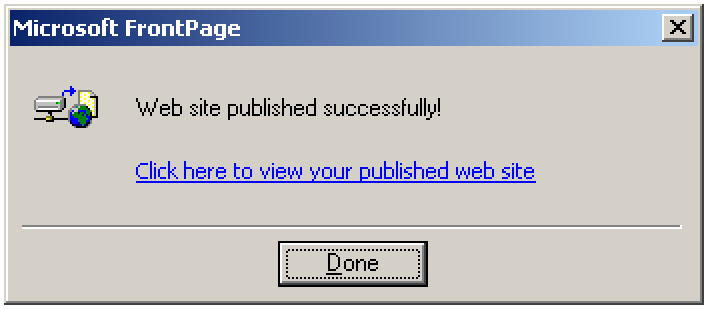
☐ Include subwebs

☑ Secure connection required (SSL)

6) In the **Specify the location to publish your web to:** box, type the location of a Web server, click the arrow to select a location to which you have published before, or click **Browse** to find the publishing location.

7) Click **Publish**.

**Note**: FrontPage publishes your web. If you want to verify that your web was successfully published, click the hyperlink that is displayed after the web has been published — your Web browser will open to the site you just published. If you cancel publishing in the middle of the operation, files that have already been published remain on the destination Web server.



Microsoft FrontPage

Web site published successfully!

Click here to view your published web site

**Tip:** To publish only pages that have changed to the same location you previously published to, click the Publish icon on the button bar.

## 7. Using Reports

All web sites require periodic maintenance. Inevitably during the process of creating and maintaining a web site, pages are created and forgotten or are deleted and the links not updated. FrontPage 2000 includes the ability to monitor the status of the added, changed and old pages, hyperlinks, page errors as well as the download speed of pages in the web. In this section we look at a couple of the important features available from the reports menu option. The items listed in this handbook should be validated every time the web is published to the NCF domain server.

a. **Unlinked Files** (better known as Orphans)

1) On the **View** menu, point to **Reports** and then click **Unlinked Files**.

b. **Broken Hyperlinks**

1) On the **View** menu, point to **Reports**, and then click **Broken Hyperlinks**.

**Note**: All broken hyperlinks in the web are listed. If a hyperlink's destination is not in the current web, the status of the hyperlink is Unknown.

2) Double-click a hyperlink with a Broken status.

3) To display the page to edit it, click **Edit Page**.

4) If you know the correct URL of the destination, edit it in the **Replace hyperlink with** box. Or, click **Browse** to browse to the page or file in a web, file system, or World Wide Web.

5) To repair other occurrences of this hyperlink in all pages in the current web, click **Change in all pages**.

6) To repair other occurrences of this hyperlink in selected pages, click **Change in selected pages**, and then select the pages.

7) Click **Replace**.

c. **Verifying Hyperlinks**

1) In **Reports** view, click **Verify Hyperlinks** on the Reporting toolbar.

2) Click **Verify all hyperlinks**, and then click **Start**.

**Note**: The status of all hyperlinks in the current web will be displayed.

## 8. Inserting Files and Objects

### a. Horizontal Lines

1) In Page view, position the cursor at a point where you want to insert a Horizontal Line.

2) Click **Insert**, **Horizontal Line**.

### b. FrontPage Components

1) **Include Page**

   a) In Page view, position the insertion point where you want to include a page.

   b) On the **Insert** menu, point to **Component**, and then click **Insert Page**.

   c) In the **Page to include** box, type the relative URL of the page to include, or click **Browse** to find the file.

### c. Pictures

1) In Page view, position the cursor at a point where you want to insert a picture.

2) Click **Insert Picture**.

3) Click **File**.

4) Browse to the picture you want from your local file system and then select the file. You can specify the type of file you want to view in the **Files of type** box.

### d. Files

1) In Page view, position the cursor at a point where you want to insert a file.

2) Click **Insert**, **File**.

3) Click **Open**.

4) Browse to the picture you want from your local file system and then select the file. You can specify the type of file you want to view in the **Files of type** box.

e. **Creating Hyperlinks**

1) In Page view, type the text you want to use as a hyperlink and then select it. For example, type and select "NCF Applications" to link to a page that describes the available NCF applications.

2) Click **Insert**, **Hyperlink**.

3) Navigate to the page to which the hyperlink will point.

4) Select **OK**.

## 9. Formatting Web Pages

You can format text in Microsoft FrontPage, as you would use a word processor, to add visual organization, emphasis, and structure. You can change the font face, size, style, color, spacing, and vertical position of text, and add effects such as underlining. You can also control spacing and indentation, add bullets and numbers, and set alignment.

a. **Set the Font for Text**

1) In Page view, select the text you want to format, right-click, and then click **Font** on the shortcut menu.

2) On the Font tab, format text by selecting options from the **Font**, **Font style**, **Size**, and **Color** boxes. You can also select one or more options under **Effects**. The Preview area shows how text looks with your settings applied to it.

b. **Bullets and Numbering**

You can create several types of lists.  In this example, we will only discuss two types.

- **Bulleted list**, for presenting a list of unordered items. A bulleted list can use the standard bullets (round, square, or circle), custom bullets that you create.

- **Numbered list**, for presenting a list of sequential items. You can choose from numbers, Roman numerals (uppercase or lowercase), or letters (uppercase or lowercase).

2) **Bulleted List**

   a) In Page view, position the insertion point where you want to create a list.

   b) On the **Format** menu, click **Bullets and Numbering**.

   c) Do one of the following:

      (1) To use standard bullets such as circles or squares, click the **Plain Bullets** tab, click the box with the bullets you want to use, and then click **OK**.

      (2) To use custom bullets, click the **Picture Bullets** tab, and click **Specify picture**. Click **Browse** to find and select the graphic you want to use. Click **OK**.

      (3) For each item you want to add to the list, type the item and then press **ENTER**. When you have typed the last item, press **ENTER** twice to end the list.

3) **Numbered Lists**

   a) In Page view, position the insertion point where you want to create a list.

   b) On the **Format** menu, click **Bullets and Numbering**, and then click the **Numbers** tab.

   c) Click the box with the style of numbers you want to use, and then click **OK**.

   d) For each item you want to add to the list, type the item and then press **ENTER**. When you have typed the last item, press **ENTER** twice to end the list.

### c. Using Shared Borders

A shared border is a region that is common to one or more pages in a web. Inside a shared border, include items that you want to appear on each page with the shared border.

#### 4) Shared Borders for a Web

a) On the **Format** menu, click **Shared Borders**.

b) Click **All pages**.

c) Select the borders (e.g. Top or Left) that you want to appear on every page in the current web.

#### 5) Shared Borders for a Page

a) In Page view, on the **Format** menu, click **Shared Borders**.

b) Click **Current page**.

c) Specify the borders that you want on this page. Shared borders are added or removed depending on your settings.

#### 1) Remove Text Formatting

You can quickly remove formatting you have applied to text. When you remove formatting, the text reverts to the default settings of its style.

a) In Page view, select the text.

b) On the **Format** menu, click **Remove Formatting**.

## 10. Creating Tables

A table is made up of rows and columns of cells in which you can insert text and graphics. When you lay out text and graphics on a page, you can use a table to arrange them. Tables are supported by virtually all Web browsers and are an easy way to layout your pages.

a. **Insert Table**

You can create a simple table just by specifying the number of rows and columns. Default properties will be used for the table. After you create a table, you can add cells, rows, and columns as needed.

- In Page view, position the insertion point where you want to insert the table.

- Click **Insert Table**, and then drag down and to the right until the number of rows and columns you want in the table is displayed.

1) **A cell**

a) In Page view, position the insertion point in a cell. On the **Table** menu, point to **Insert**, and then click **Cell**. A new cell is inserted to the left of the cell.

2) **A row**

a) In Page view, select a row. On the **Table** menu, point to **Insert**, and then click **Rows or Columns**. Click **Rows**, enter the number of rows to insert, and specify where to place them.

3) **A column**

a) In Page view, select a column. On the **Table** menu, point to **Insert**, and then click **Rows or Columns**. Click **Columns**, enter the number of columns to insert, and specify where to place them.

4) **Captions**

a) In Page view, position the insertion point in the table. On the Table menu, point to Insert, and then click Caption. Type the text for your caption.

b. **Selecting Cells**

1) **A table**

a) In Page view, click anywhere in the table. Point to **Select** on the **Table** menu, and then click **Table**. Or, move the mouse pointer to the left of the table, and then double-click when the mouse pointer changes to an arrow.

2) **A cell**

   a) In Page view, position the insertion point in a cell, point to **Select** on the **Table** menu, and then click **Cell**. Or, press and hold **ALT**, then click the **cell**.

   b) To select multiple adjacent cells, click and drag the mouse pointer over the cells. To select noncontiguous cells, press and hold **SHIFT**, then click the **cells**.

3) **A row**

   a) In Page view, move the mouse pointer over the left border of the row, and then click when the mouse pointer changes to an arrow. To select multiple rows, drag the mouse pointer over the rows.

4) **A column**

   a) In Page view, move the mouse pointer over the top border of the column, and then click when the mouse pointer changes to an arrow. To select multiple columns, drag the mouse pointer over the columns.

5) **A table caption**

   a) In Page view, move the mouse pointer to the left of the caption, and then click when the pointer changes to an arrow. Or, press and hold **ALT**, and then click the **caption**.

## 11. Modifying Object Properties

### a. Font Properties

1) In Page view, select the text you want to format, **right-click**, and then click **Font** on the shortcut menu.

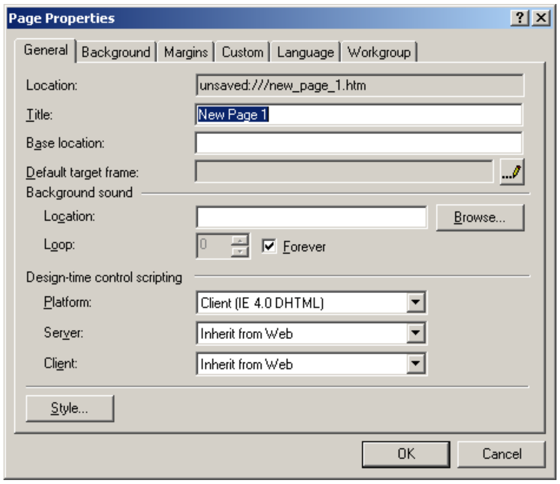
2) On the Font tab, format text by selecting options from the **Font**, **Font style**, **Size**, and **Color** boxes. You can also select one or more options under **Effects**. The Preview area shows how text looks with your settings applied to it.

## b. Page Properties

### 1) General Tab

a) In Page view, **right-click** the page, click **Page Properties** on the shortcut menu, and then click the **General** tab.

b) In the **Title** box, enter the page title.



Page Properties

Location: unsaved:///new_page_1.htm

Title: New Page 1

Base location:

Default target frame:

Background sound

Location:

Loop: 0 ☑ Forever

Design-time control scripting

Platform: Client (IE 4.0 DHTML)

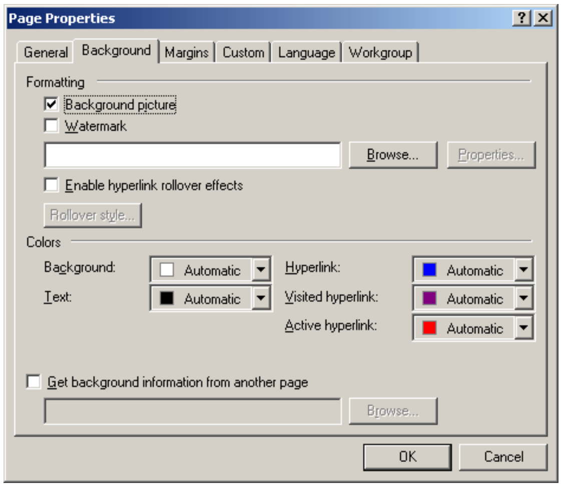
Server: Inherit from Web

Client: Inherit from Web

### 2) Background Tab

a) In Page view, **right-click** the page, click **Page Properties** on the shortcut menu, and then click the **Background** tab.

b) In the **Background** box, select a background color.



Page Properties

Formatting

☑ Background picture

☐ Watermark

☐ Enable hyperlink rollover effects

Colors

Background: □ Automatic

Text: ■ Automatic

Hyperlink: 🟦 Automatic

Visited hyperlink: 🟪 Automatic

Active hyperlink: 🟥 Automatic

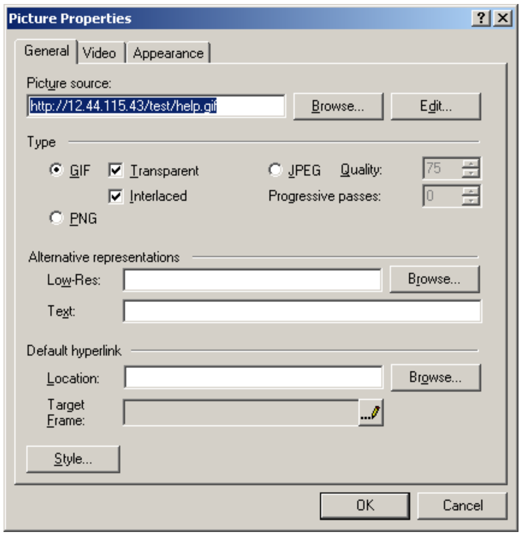
☐ Get background information from another page

## c. Picture Properties

### 1) Image

a) In Page view, **right-click** the picture, and then click **Picture Properties** on the shortcut menu.

b) On the **General** tab, if the picture is in GIF format, you can specify whether the picture should be interlaced by selecting **Interlaced**. If a transparent color has been set, the **Transparent** box is selected; you can remove the transparency by clearing this box.


Picture source: http://12.44.115.43/test/help.gif

● GIF ☑ Transparent ☑ Interlaced

○ PNG

○ JPEG Quality: 75

Progressive passes: 0

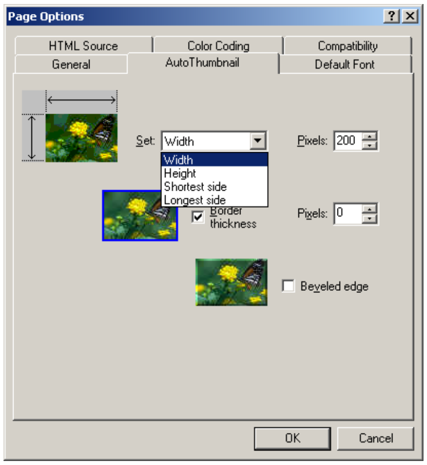
c) If the picture is in JPEG format, you can specify the quality of the JPEG by entering a value from 1 to 100 in the **Quality** box.

### 2) Image Thumbnails

a) On the **Tools** menu, click **Page Options**, and then click the **AutoThumbnail** tab.

(1) In the **Set** box, click the option you want to use for specifying a size, then in the **Pixels** box, enter the value in pixels.

For example, if you want thumbnail pictures to be 75 pixels wide, click Width and then enter 75. The height of the thumbnail will be sized to maintain the proportions (aspect ratio) of the original picture. Or, if you select **Shortest side** and then enter 75, the shortest side of any


Set: Width

Pixels: 200

☑ Border thickness Pixels: 0

□ Beveled edge

thumbnail picture, whether height or width, will be 75 pixels.

(2) To specify a border, select **Border thickness**, and then in the **Pixels** box, enter a value for the thickness of the border in pixels.

(3) If you want the graphic to be beveled, select **Beveled edge**. If you have also specified a border thickness, the thumbnail will have a beveled edge inside of a border.

## d. Adjusting Tables and Cell Properties

### 1) Table

a) In Page view, **right-click** the table, and then click **Table Properties** on the shortcut menu.

b) In the **Alignment** box, select the alignment to use for the table.

c) In the **Float** box, specify whether you want text to flow around the left or right of the table. If you do not want text to flow around the table, select **Default**.

d) Under **Borders**, in the **Size** box, enter the width of the border in pixels.

e) In the **Cell padding** box, enter how much space to allow between the contents and inside edges of cells, in pixels.

f) In the **Cell spacing** box, enter how much space to allow between the cells in the table, in pixels.

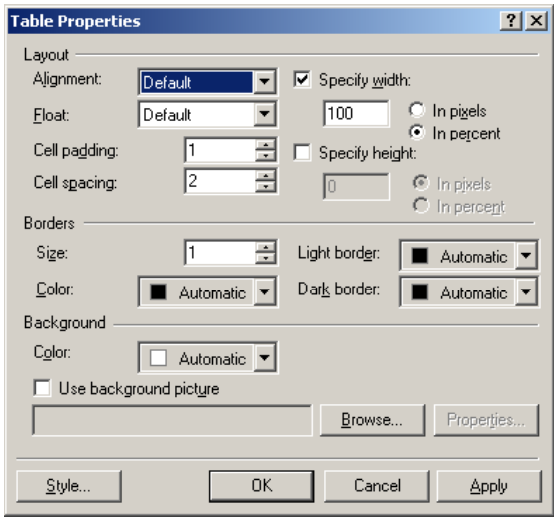


Table Properties

Layout

Alignment: Default

☑ Specify width: 100 ○ In pixels ● In percent

Float: Default

Cell padding: 1

☐ Specify height: 0 ● In pixels ○ In percent

Cell spacing: 2

Borders

Size: 1

Light border: ■ Automatic

Color: ■ Automatic

Dark border: ■ Automatic

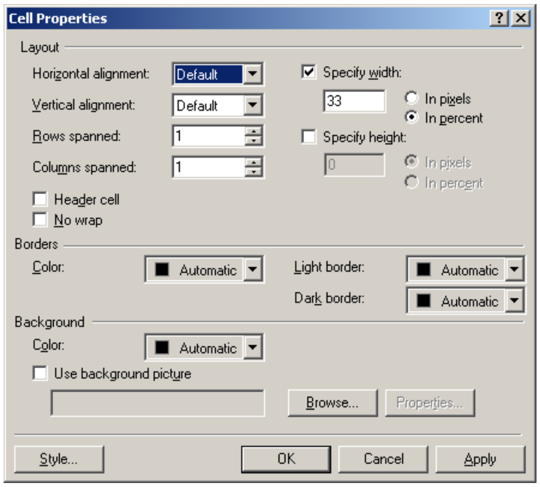
Background

Color: □ Automatic

☐ Use background picture

2) **Cell**

a) In Page view, select the cells for which you want to set the layout.



Layout

Horizontal alignment: Default

Vertical alignment: Default

Rows spanned: 1

Columns spanned: 1

□ Header cell

□ No wrap

☑ Specify width: 33

○ In pixels

● In percent

□ Specify height: 0

● In pixels

○ In percent

Borders

Color: ■ Automatic

Light border: ■ Automatic

Dark border: ■ Automatic

Background

Color: ■ Automatic

□ Use background picture

b) **Right-click**, and then click **Cell Properties** on the shortcut menu.

c) In the **Horizontal alignment** and **Vertical alignment** boxes, select the alignment you want for the contents of the cell.

d) To set the cells as header cells and emphasize them, select **Header cell**. By default, the emphasis is bold text.

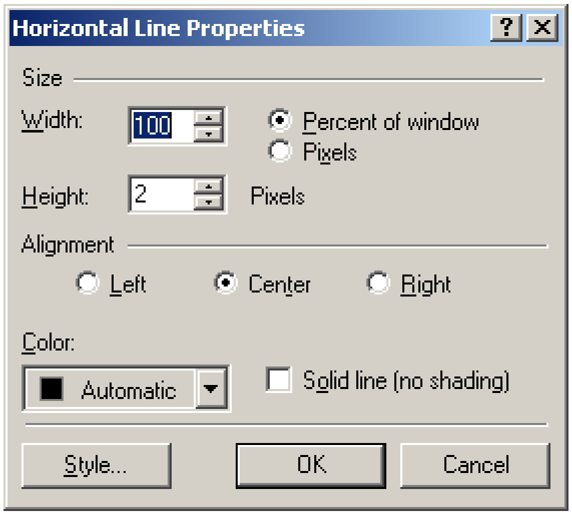
e) To prevent Web browsers from wrapping text in the cell, select **No wrap**.

3) **Caption**

a) To position the caption below the table, **right-click** the caption, and then click **Caption Properties** on the shortcut menu.

b) Click **Bottom of table**, and then click **OK**.

e. **Horizontal Line**



Size

Width: 100

● Percent of window

○ Pixels

Height: 2 Pixels

Alignment

○ Left ● Center ○ Right

Color: ■ Automatic

□ Solid line (no shading)

1) In Page view, **double-click** the **Horizontal Line** to edit.

2) Under **Width**, specify the width of the line as a percentage of the window width or as a number of pixels.

3) Under **Height**, enter the number of pixels high the line

should be.

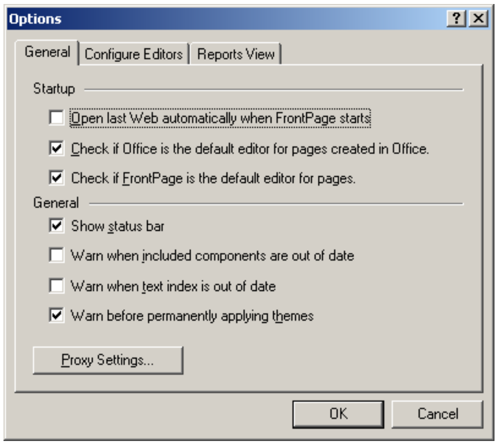
4) Under **Alignment**, specify the alignment of the line on the page.

5) In the **Color** box, select a color for the line if you do not want a shaded line.

6) Select the **Solid Line** check box if you want the line to appear solid. Clear the check box if you want the line to appear shaded. If you select a color, the line will be solid, and you cannot apply shading.

## 12. Spell Checking Documents

### a. As you type



Startup

☐ Open last Web automatically when FrontPage starts

☑ Check if Office is the default editor for pages created in Office.

☑ Check if FrontPage is the default editor for pages.

General

☑ Show status bar

☐ Warn when included components are out of date

☐ Warn when text index is out of date

☑ Warn before permanently applying themes

1) On the **Tools** menu, click **Page Options**.

2) On the **General** tab, select the **Check spelling as you type** check box.

3) If you don't want misspelled words to be underlined, select the **Hide spelling errors in all documents** check box. To show spelling errors, clear this check box.

### b. In a Web

1) Switch to **Folders** view.

**Note**: If you do not want to check spelling on each page in the web, select the pages you want to check.

2) Click **Spelling**.

3) Select one of the following:

a) **Entire web**; To check spelling in all pages in the current web.

b) **Selected pages**; To check spelling in pages you have selected.

4) Click **Start**. (When FrontPage lists the pages with misspelled words, do the following:)

   a) **Double-click** a page.

   b) FrontPage opens the page in Page view and prompts you to correct the misspelled words.

   c) When you have reviewed all occurrences of the text on the page, you are prompted to save and close the page.

   d) Continue to the next page on which a misspelling was found.

c. **In a Page**

1) In Page view, click **Tools**, **Spelling**.

2) If an unrecognized word is found, the Spelling dialog box opens, and displays the word in the **Not in Dictionary** box.

3) Do one of the following: To replace the misspelled word with a word from the **Suggestions** list, click the **suggested word**, and then click **Change**. Click **Change All** to correct all instances of this word.

4) To correct the word yourself, type the correct word in the **Change To** box, and then click **Change**. Click **Change All** to correct all instances of this word.

5) If the unrecognized word is correctly spelled, click **Ignore** to ignore this instance of the word, or click **Ignore All** to ignore all instance of this word. Click **Add** to add the word to your custom dictionary.

## 13. Keyboard Short Cuts

The table below identifies keyboard shortcuts available in Microsoft FrontPage 2000.

### a. Keys for working with pages

| **To** | **Press** |
|---|---|
| Create a new page | CTRL+N |
| Open a page | CTRL+O |
| Create a hyperlink on a page | CTRL+K |

| | |
|---|---|
| Preview a page in a Web browser | CTRL+SHIFT+B |
| Print a page | CTRL+P |
| Display non-printing characters | CTRL+ SHIFT+8 |
| Display HTML tags | CTRL+ / |
| Refresh a page | F5 |
| Switch between open pages | CTRL+TAB<br>CTRL+SHIFT+TAB |
| Close a page | CTRL+F4 |
| Save a page | CTRL+S |
| Quit Microsoft FrontPage | ALT+F4 |
| Find text on pages or in HTML | CTRL+F |
| Replace text on pages or in HTML | CTRL+H |
| Check spelling on a page | F7 |
| Look up a word in the Thesaurus | SHIFT+F7 |
| Cancel an action | ESC |
| Undo an action | CTRL+Z<br>or ALT+BACKSPACE |
| Redo or repeat an action | CTRL+Y<br>or SHIFT+ALT+BACKSPACE |

### b. Keys for formatting text and paragraphs

| **To** | **Press** |
|---|---|
| Change the font | CTRL+SHIFT+F |
| Change the font size | CTRL+SHIFT+P |
| Apply bold formatting | CTRL+B |
| Apply an underline | CTRL+U |
| Apply italic formatting | CTRL+I |
| Apply superscript formatting | CTRL+PLUS SIGN |
| Apply subscript formatting | CTRL+MINUS SIGN |

| | |
|---|---|
| Copy formatting | CTRL+ SHIFT+C |
| Paste formatting | CTRL+SHIFT+V |
| Remove manual formatting | CTRL+SHIFT+Z<br>or CTRL+SPACEBAR |
| Center a paragraph | CTRL+E |
| Left align a paragraph | CTRL+L |
| Right align a paragraph | CTRL+R |
| Indent a paragraph from the left | CTRL+M |
| Indent a paragraph from the right | CTRL+ SHIFT+M |
| Apply a style | CTRL+ SHIFT+S |
| Apply the Normal style | CTRL+SHIFT+ N |
| Apply the Heading 1 style | CTRL+ALT+1 |
| Apply the Heading 2 style | CTRL+ALT+2 |
| Apply the Heading 3 style | CTRL+ALT+3 |
| Apply the Heading 4 style | CTRL+ALT+4 |
| Apply the Heading 5 style | CTRL+ALT+5 |
| Apply the Heading 6 style | CTRL+ALT+6 |
| Apply the List style | CTRL+ SHIFT+L |

### c. Keys for editing and moving text and graphics

| **To** | **Press** |
|---|---|
| Delete one character to the left | BACKSPACE |
| Delete one character to the right | DELETE |
| Delete one word to the left | CTRL+BACKSPACE |
| Delete one word to the right | CTRL+DELETE |
| Cut selected text to the clipboard | CTRL+X<br>or SHIFT+DELETE |
| Copy text or graphics | CTRL+C<br>or CTRL+INSERT |

| | |
|---|---|
| Paste the clipboard contents | CTRL+V<br>or SHIFT+INSERT |
| Insert a line break | SHIFT+ENTER |
| Insert a nonbreaking space | CTRL+SHIFT+SPACEBAR |

### d. **Keys for selecting text and graphics**

| **To extend a selection** | **Press** |
|---|---|
| One character to the right | SHIFT+RIGHT ARROW |
| One character to the left | SHIFT+LEFT ARROW |
| To the end of a word | CTRL+SHIFT+RIGHT ARROW |
| To the end of a line | SHIFT+END |
| To the beginning of a line | SHIFT+HOME |
| One line down | SHIFT+DOWN ARROW |
| One line up | SHIFT+UP ARROW |
| To the end of a paragraph | CTRL+SHIFT+DOWN ARROW |
| To the beginning of a paragraph | CTRL+SHIFT+UP ARROW |
| One screen down | SHIFT+PAGE DOWN |
| One screen up | SHIFT+PAGE UP |
| To include the entire page | CTRL+A |
| Display the properties of a selection | ALT+ENTER |
| Insert a table | SHIFT+CTRL+ALT+T |
| Select the next cell's contents | TAB |
| Select the preceding cell's contents | SHIFT+TAB |
| Extend a selection to adjacent cells | Hold down SHIFT and press an arrow key repeatedly |
| Select a column | Click in the column's top or bottom cell,<br>then hold down SHIFT and press the<br>UP ARROW or DOWN ARROW key repeatedly |

### e. **Keys for menus and toolbars**

| **To** | **Press** |
|---|---|
| Show the shortcut menu | SHIFT+F10 |
| Make the menu bar active | F10 |
| Show the program icon menu | ALT+SPACEBAR |
| Select the next or previous command on the menu or submenu | DOWN ARROW or DOWN ARROW (with the menu or submenu displayed) |
| Close the visible menu and submenu at the same time | ALT |
| Close the visible menu; or, with a submenu visible, close the submenu only | ESC |
| Create an Auto Thumbnail of a selected picture | CTRL+T |

### f. **Keys for Help**

| **To** | **Press** |
|---|---|
| Display the online Help | F1 |
| Display context-sensitive Help | SHIFT+F1 |

# Chapter 6

## NCF Intranet Applications

This page left intentionally blank

Overview

Chapter 6 provides a brief overview of the applications either available or in development for the NCF. This chapter is not intended to provide detailed instructions or step-by-step guidelines on how to use.

Online applications serve multiple purposes. Two of which are: 1) Streamline the business practices with-in the NCF and 2) making the application available globally. On-line applications considerably simplify the submission process for common things like submitting awards to the Brigades for action or managing IT inventories for all our Units. They simplify the administrative processes for other task-orientated jobs like submitting photos, changing passwords or centrally locating Command instructions. Below is a brief description of the available applications as well as those in development.
Access to all NCF application is available at http://ncf.navfac.navy.mil/apps.htm

## 1. User Manager

The application allows users to remotely, via a web page, to update their user account /s. Users are notified via email with-in 15 days of account expiration. Notification is sent daily during the 15-day period until the account is updated. If the account is no longer required, the NCF Webmaster should be notified so it may be disabled.
The primary Unit Webmaster will be notified when the Friends and Family account is due to expire.

## 2. Document Library

The Document Library provides a central storage area for all Unit instructions, notices, and MOU's. Users can search for documents in one of two ways, either by All Commands or by individual Commands. The application is available to all NCF Units. Those requesting access should contact the NCF Webmaster.

## 3. Photo Library

Photo Library is an application that provides a means for the PAO's to post pictures of Seabees at work to the NCF Internet homepages. The application cycles though the available photos every 25 seconds. Access to the application should be requested through the NCF Webmaster.

## 4. Awards

The Awards application although still in beta should be ready shortly. The application tracks the submission process of awards from the Units to the Brigades. To submit an award, users will complete the on-line 1650 and submit it.

## 5. IT Inventory

The IT Inventory application is currently in development at the time of this writing; it will provide a means on managing all Brigade IT assets via the web. The applications functionality allows asset tracking, management and reporting.

## 6. Project Management / OPS Reporting

The OPS application is designed to exclusively manage all NCF projects abroad. Some of the functionality requested of the application but not limited to:

- Establish access for Brigade Operations Staff to create projects, enter and edit general project information, assign projects to units, delete or suspend projects, assign initial manday tasking, revise manday tasking, cancel manday tasking, access standard reports, and create custom queries.

- Establish access for Second Echelon NCF Units to update project status including work in place (WIP) percentage and mandays expended, create monthly SITREP input report, access standard reports, and create custom queries.

- Establish access for all NCF Intranet users to view standard reports.

- Establish a process for tracking material acquisition and receipts.

# Chapter 7

## Web Management on the NCF Corporate Intranet

This page left intentionally blank

## 1. Overview

The NCF Intranet is a tool like any other we use to execute our duties. Just as we strive to organize our projects or office spaces, so should we manage our Web sites with due diligence. The only difference for our Web sites is that outside entities are looking at the information we provide. Web sites should be organized logically so anyone outside our organization can find the information – data is useless if no one can find it.

*Main topic* areas should be organized into folders, whereas archived information (e.g. documents, reports, briefs, etc.) should be placed in an archive folder identifying it as "archived information." The ultimate goal is placing information in specific locations and never moving it again. (**Note:** Information should be easy to find and readily identifiable by all users. Navigation should always be kept to a minimum throughout any Web site.)

The concept behind the Web site templates is, regardless of which Web site the user is on, similar information will be in the same relative location.

Some NCF Webmasters administer centralized Web sites; camp Web sites are an example. Relocating information and files within these specific sites can break hyperlinks from other Web sites, namely those of the Battalions.

Another administrative task is regular maintenance, which includes validating hyperlinks, removing or re-linking orphaned files, and ensuring file and folder names adhere to naming conventions (no spaces or special characters). If files are located in folders with no associated links, they should either be removed or re-linked. (**Note:** As the case with pictures; they typically reference a specific event in time and are needed for no other purpose.) When the page is removed, the pictures are typically left in the folder unnoticed. This can create problems for publishers and the Server Extensions, as well as increasing the time required to backup the system.

Web sites require periodic housecleaning, purging temporary information that is no longer needed. Note, this does not include reports, briefs, inventories, etc. These items shall always be archived and referenced from a page. Pages that are published with the intent of remaining for short periods of time should be placed in folders that identify them as temporary to key the Webmaster to periodically review the content for relevancy.

Ideally information should be categorized and located in appropriate folders (e.g. reports, SITREPs, briefs, etc.) and converted to pdf format or, as with PowerPoint presentations, converted to HTML. All other information not requiring any changes should be archived and stored accordingly. Native file formats (e.g. .doc, .xls, .ppt) should rarely be made accessible from the web. They have the potential to cause compatibility problems for Web browsers.

PowerPoint presentations should be saved as HTML or pdf and not posted in their native format (ppt or pps). If the presentation is to be posted for a brief period of time and the intent is to have the user download, it should it be packed into a zip file. Saving PowerPoint presentations as HTML with the use of Frames causes problems as well, trapping the user in the frame. (**Note:** The only way out of a frame is to replace the URL in the browser address bar or continually click the back button.) If there's a specific reason to use a frame, always set the link to "open in a new window" so it may be closed and the user may then return to the Web site.

Some sites are managed online, although this practice is discouraged. Sites with multiple managers can fall into this category. Managing a web in this fashion is somewhat unavoidable only because more than one publisher is updating the Web site and the possibility exists to overwrite the others' work. The problem is if a mistake is made, the mistake is online instantaneously with no ability to proofread the information first; therefore managing sites online should be avoided whenever possible.

The NAVFAC Style guide provides Webmasters with an administration guide as well as the requirements [font type, size, protocols, supported applications (e.g. cfm and html), etc] adopted by the NCF. It sets the standard for both the NAVFAC Corporate and NCF Intranets. The information is available from the NAVFAC Intranet Web site (http://navfacilitator.navfac.navy.mil/about/) or follow the "About the Intranet" hyperlink in the NAVFAC banner.

Proper Web site management reduces the amount of administration required in the long run, simplifies turnovers, and ensures every deployment site is like the others.

## 2. Standardization of posted information

As mentioned earlier, the NCF Intranet / Internet Web site templates were created with the notion that information would be referenced in the same typical manner from one Web site to another. For example, you can readily find Company information on the home page of all Unit intranet Web sites. All Units within the NCF at one time or another have had requirements to resource historical information. What better place for this information than on the Web where everyone has access.

The initial concept of the Web site templates was to create a common set of links on the home pages that would point to tables on other pages. Within these tables, links would reference dated information that would reach back to the creation of the Web site and beyond, if available. Since the nature of our business is the same for all like Units, it made sense that the information stores be similar; therefore depending on the Web site visited, the user could be assured of finding the same type of information for any given Unit.

It’s understandable that each Unit prefers to manage their Web sites in their own fashion. But if each Unit implements their own definition of “easy navigation,” others who need to access the information may find themselves spending countless hours searching for information. Like everything we do, there needs to be some standardization in which all Web sites are organized. The template was only a starting point and not necessarily the final result. Although the current templates are the only version approved by the NCF ESG, this is not to say there cannot be changes. Part of the tasking for the Webmaster Conference is to recommend changes to the standard template design, which will be briefed at the next C4I QMB.

Camp Web sites should store information generated on deployment with hyperlinks from Command Web sites. Do not physically store deployed information in Command Webs. Information stored on the Command webs should be specific to the Unit and not the deployment site.

The problem that currently exists as explained in the section above is a new Webmasters comes on-board without any knowledge of the Unit’s past and makes decisions about what is or is not pertinent within the Web site. As soon as the information is deleted, it’s gone forever. This is something we cannot afford to happen, which is exactly why placing all information generated on deployment (SITREPs, briefs, inventories, etc) to the camp Web sites is so important. Here, the information will be stored forever or as long as the web servers exist. There’s no reason to delete the archived information within these webs.

Command Web sites should contain Unit specific information. Contact lists for all staff personnel with e-mail addresses; pages with links to SITREPS, reports, and other information generated while on deployment; as well as any reports or information generated while in homeport [# of SCWS qualified personnel, training lists, and plans for the person (if still generated)]. If the Unit is in homeport and generating reports, those pages should reside on the Command Web site. Most important though, all Units should be generating the same type of information and posting it in the same relative location.

### 3. Effective management of Camp Web sites

Historically, requesting archived information from Units is time consuming and cumbersome. The NCF Intranet satisfies many requirements with regards to recovering information past, present, and future and will continue to be a valuable resource.

The Camp Web site’s sole purpose is to store all information, transactions, and events that occur on any given deployment site, including details and detachments. It is crucial to the success of our business that these Web sites standardize on a template. Every mainbody deployment site produces the same information. Geographic location is the only major difference.

The Web sites should be organized so information is easily accessible. The home page identifies the Camp OIC and their contact information. Commanding Officer information of the resident Battalion was recently added to better identify who is currently on-board.

Because the home page is normally the first page accessed when visiting a Web site, a bulletin board is available to post new and/or important information with links to pages with more detail (e.g. monthly reoccurring reports, etc.). The links should point to a page that lists all reports for that category, sorted chronologically. For example, view any of the QMB Web sites -- this is exactly how they are to be organized.

The banners are managed by the NCF Webmaster and distributed to the Units who have Intranet Web sites. The banners not only identify the Unit but also which camps they deploy to; similarly, the camp banner identifies the four Battalions in a deployment rotation to that location. These banners are not to be altered by the Unit Webmasters, as this is an approved item from the NCF ESG. If changes are required or recommended, they should be brought to the attention of the NCF Webmaster for NCF C4I QMB approval.

The Links on the right-hand side of the home page will direct visitors to a set of standard information. The following is an example of the standard set of links:

- **Points of Contact** – Phone listing by office code.

- **Camp Information** – General information about the Camp (Office photos, Camp topology, directions, etc).

- **S1 Admin/ Personnel** – Reports generated while on deployment, information pertinent to turnover.

- **S3 Operations** – Monthly SITREPS, photo SITREPS, Level Ones, project information, CESE inventories and equipment status, etc.

- **S4 Supply** – MLO status reports, financial reports, information pertinent to turnover.

- **S6 Comms/ IS** – COMM and IS inventories, status of equipment, information pertinent to turnover.

- **S7 Training** – Armory inventories, status of equipment, information pertinent to turnover.

- **Archived Reports** – Multiple links to pages illustrating specific reports.

- **MWR/ Service Outlets** – Resources for Unit personnel as well as incoming Units with information about the area, services available in camp and surrounding bases, and off duty activities.

A basic Web site structure would consist of a home page (primary tier), categorical pages (secondary tier), and category details (tertiary tier).

The home page provides general information, a set of links to the main departments, and simplifies navigation throughout the site.

The secondary pages should either provide the desired information, additional options to navigate from, or tables providing links to detailed information.

Table columns may be organized as follows:

| FY 99 | FY 00 | FY 01 |
|---|---|---|
| March | April | Aug |
| April | May | Oct |

(Although this method is not a requirement, it simply illustrates a means of organizing the web pages whereby simplifying the navigation.)

The tertiary pages would contain the detailed information or reports.

All information posted on the camp Web sites is linkable from all other Web sites. No information should be stored twice. Multiple instances of a file expend valuable resources on the servers and increase the potential for outdated information.

If the resident Battalion feels the need to have ownership of the information posted on the Camp Web sites, another option may be to create folders for each Unit and a folder structure beneath it. It would look something like this:

- NMCB4
    - S1
    - S3
        - Alfa
            - Operations
            - Maintenance
        - Bravo
            - Projects
            - Camp_Maintenance
        - Charlie
        - Delta
        - Detachments
    - S4

- S6
    - S7
    - Archived_Reports

- NMCB7
    - Same folder structure

This feature would identify the Unit (within the URL) who is responsible for the information.

At any rate the information has to be stored in a similar manner from one site to the next to eliminate confusion and the lengthy navigation from one site to another.

Commands should provide links to the Camp Web sites, illustrating the information they posted or acknowledging the work they have accomplished.

## Notes:

DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

DEC 7 1998

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR OF ADMINISTRATION AND MANAGEMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Web Site Administration

This memorandum provides the DoD policy, assigns responsibility, and describes the procedures for establishing, operating and maintaining DoD unclassified Web sites. DoD is committed to maximizing the availability of timely and accurate Defense information to the public as well as maintaining a secure framework for our use of Internet-based technologies. At the same time, we must be continually mindful of our responsibility to protect our most precious resource–our men and women who serve this Nation, and their families.

To accomplish the above, all DoD Components have the responsibility to ensure sound information assurance practices are in place and operating for Web sites. Heads of Components shall be responsible for managing the use and content of the information placed on the Web consistent with the guidance and processes contained in the attached. This memorandum cancels the joint ASD (PA) and ASD (C3I) memorandum entitled "Establishing and Maintaining a Publicly Accessible Department of Defense Web Information Service," and dated July 18, 1997 (as amended).

In view of the changing environment and the impact of information technology on the sensitivity of information, I further direct that within the next 120 days:

- The DoD General Counsel lead a review of statutes as they relate to our ability to safeguard sensitive, unclassified information and advise me of any recommended changes;

- The Director Administration and Management lead a review of "privacy-related" policies, and release of information to ensure that we are maintaining the proper balance with respect to individuals' privacy;

- The USD (A&T) lead a review of the Department's ability to safeguard sensitive, unclassified information in our electronic commerce systems.

I further direct that the Senior Civilian Official OASD(C3I), working with the ASD (PA) and the Director of Administration and Management ensure that the web site administration policy and procedures are codified in the DoD Publication System within 120 days.

Comments, suggestions and recommendations for changes to the attached policy and guidance should be directed to OASD(C3I). An electronic copy of this guidance is available at http://www.defenselink.mil/admin/about.html#WebPolicies.

John J Hamre

John J. Hamre

Attachment

# Web Site Administration

# Policies & Procedures

**November 25, 1998**

Office of the Assistant Secretary of Defense
(Command, Control, Communications & Intelligence)
6000 Defense Pentagon
Washington, DC  20301-6000

# Department of Defense
# WEB SITE ADMINISTRATION GUIDANCE

## CONTENTS

**DEPSECDEF Memorandum Subject: Web Site Information Services DoD-Wide, dated November 25, 1998 implements the policies, responsibilities and procedures for Web Site Administration. An electronic copy of this guidance is available at http://www.defenselink.mil/admin/about.html#WebPolicies. Please forward comments, suggestions and recommendations for changes to: OASD (C3I), ODASD (Policy & Implementation/Deputy CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.**

# WEB SITE ADMINISTRATION

## Part I – Policy & Responsibilities

November 25, 1998

1. PURPOSE

This document delineates the policy and assigns responsibility related to establishing, operating and maintaining unclassified Web sites and other related services. It supersedes the "Guidelines for Establishing and Maintaining a Publicly Accessible Department of Defense Web Information Service" jointly published by the Office of the Assistant Secretary of Defense (Public Affairs) and the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) on July 18, 1997 (updated January 9, 1998).

2. APPLICABILITY

This policy applies to:

2.1. The Office of the Secretary of Defense (OSD), the Military Departments (including the Coast Guard when it is operated as a Military Service in the Navy), the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Defense Agencies, and the Department of Defense (DoD) Field Activities (hereafter referred to collectively as "the DoD Components") and to their contractors and consultants including those who operate or maintain DoD Web sites for them, through incorporation into contracts.

2.2. All unclassified DoD Web sites, both publicly and non-publicly accessible.

2.3. Reviewing approval requests received from DoD contractors and subcontractors relative to the posting of unclassified DoD information to a DoD contractor Web site.

3. DEFINITIONS

Terms used in this document are defined in Part III.

4. POLICY

It is the policy of the DoD that:

4.1. Using the World Wide Web is strongly encouraged in that it provides the DoD with a powerful tool to convey information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies and programs.

4.2. The considerable mission benefits gained by using the Web must be carefully balanced through the application of comprehensive risk management procedures against the potential risk to DoD interests, such as national security, the conduct of federal programs, the safety and security of personnel or assets, or individual privacy created by having electronically aggregated DoD information more readily accessible to a worldwide audience.

4.3. Each organization operating a DoD Web site will implement technical security best practices with regard to its establishment, maintenance and administration.

4.3.1. DoD Web sites containing i) FOR OFFICIAL USE ONLY information, ii) information not specifically cleared and marked as approved for public release in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29 (references (h) and (o)), or iii) information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to the DoD, especially in electronically aggregated form, must employ additional security and access controls. Web sites containing information in these categories should not be accessible to the general public.

4.4. Consistent with other leadership responsibilities for public and internal communication, the decision whether or not to establish an organizational Web site, and to publish appropriate instructions and regulations for a Web site within the limitations established by this document, is hereby delegated to each DoD Component.

## 5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD (C3I)) shall:

5.1.1. Provide policy and procedural guidance with respect to establishing, operating and maintaining Web sites.

5.1.2. Maintain liaison with the Assistant Secretary of Defense for Public Affairs to provide policy oversight and guidance to ensure the effective dissemination of defense information via the Internet.

5.1.3. Provide technical support consistent with existing Chief Information Officer (CIO) responsibilities.

5.1.4. Develop and maintain, in coordination with the Chairman of the Joint Chiefs of Staff, Under Secretary of Defense (Personnel &Readiness), and General Counsel, training guidance and requirements that addresses information security on the Web.

5.1.5. Approve and publish DoD Instructions and Publications, as necessary, to guide, direct, or help Web site activities, consistent with DoD 5025.1-M (reference (kk)).

5.1.6. Provide a mechanism for feedback reporting across DoD, to include "Lessons Learned" and the identification of useful automated tools to aid in the conduct of multi-disciplinary security assessments of Web sites.

5.1.7. Ensure compliance with this policy.

5.2. The Assistant Secretary of Defense for Public Affairs (OASD (PA)) shall:

5.2.1. Operate and maintain DefenseLINK (http://www.defenselink.mil) as the official primary point of access to DoD information on the Internet.

5.2.2. In coordination with the other OSD Principal Staff Assistants, provide oversight policy and guidance to ensure the absolute credibility of defense information released to the public through publicly accessible Web sites.

5.2.3. Establish and maintain a central Web site registration system for the Department that meets the requirements for the Government Information Locator Service (GILS) and is integrated with Service-level registration systems.

5.3. The Assistant Secretary of Defense for Reserve Affairs and the Chairman of the Joint Chiefs of Staff shall develop and implement a plan that uses Reserve Component assets to conduct ongoing operations security and threat assessments of Component Web sites.

5.4. The Secretaries of the Military Departments shall establish and maintain a central registration system for the respective service that meets the requirements for GILS and is integrated with DefenseLINK.

5.5. The Heads of the DoD Components shall:

5.5.1. Establish a process for the identification of information appropriate for posting to Web sites and ensure it is consistently applied.

5.5.2. Ensure all information placed on publicly accessible Web sites is properly reviewed for security, levels of sensitivity and other concerns before it is released. Detailed requirements for clearance of information for public release are located in DoD Directive 5230.9 and DOD Instruction 5230.29 (references (h) and (o)) and Part II of this document.

5.5.3. Ensure approved DoD security and privacy notices and applicable disclaimers are used on all Web sites under their purview.

5.5.4. Ensure all information placed on publicly accessible Web sites is appropriate for worldwide dissemination and does not place national security, DoD personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk.

5.5.5. Ensure procedures are established for management oversight and regular functional review of the Web site.

5.5.6. Ensure operational integrity and security of the computer and network supporting the Web site is maintained.

5.5.7. Ensure that reasonable efforts are made to verify the accuracy, consistency, appropriateness, and timeliness of all information placed on the Web site.

5.5.8. Register each publicly accessible Web site with the Government Information Locator Service (GILS).

5.5.9. Provide the necessary resources to adequately support Web site operations to include funding, equipping, staffing and training.

5.5.10. Ensure that a comprehensive, multi-disciplinary security assessment is conducted of their Web sites within 120 days of the promulgation of this document, and at least annually thereafter.

5.5.11. Provide a mechanism for feedback reporting within the Component, to include "Lessons Learned" suitable for all DoD Components.

5.5.12. Ensure compliance with this policy for those functions, missions, agencies, and activities in their purview.

5.5.13. Grant waivers on a non-delegable basis to a provision of the procedures contained in Part II of this document when it has been determined that immediate implementation would adversely impact essential mission accomplishment. Instances where such waivers have been granted will be reported to the Assistant Secretary of Defense (C3I).

6. EFFECTIVE DATE. This policy is effective immediately.

# WEB SITE ADMINISTRATION

## Part II – Procedures

November 25, 1998

1. PURPOSE

This document delineates the processes and procedures related to establishing, operating and maintaining unclassified Web sites and other related services. It also provides guidelines for the review of material prior to its posting to Web sites.

2. WEB SITE ESTABLISHMENT

2.1. Support of Mission. Each Web site shall have a clearly defined purpose that supports the mission of the DoD Component. The Head of the DoD Component, or his/her designee in accordance with official policies, shall approve the defined purpose and general content of the Web site. Non-copyrighted material, text, clip art, hypertext links, images and sound or video clips may be used only if they directly relate to the Component's mission.

2.2. Web Site Security Accreditation. Each organization establishing a Web site shall institute a security certification and accreditation procedure in accordance with DoD Directive 5200.40 (Reference (v)). Successful implementation depends on defining security requirements early in the process of establishing a Web site. All security-related disciplines (computer, communications, personnel, etc.) shall be considered in the requirements definition for the Web site. Cost versus risk tradeoffs shall be evaluated and security requirements assigned accordingly.

2.3 Single Source Information. For the purpose of preventing duplication on the Web, a Web site shall normally be limited only to information for which the establishing organization is responsible. Web sites that contain information pursuant to the requirements of the Electronic Freedom of Information Act, 5 USC 552(a)(2)(D) & (E) (reference (j)) are exempt from this restriction. Information from other sources on the Internet will not be copied but will be referenced or otherwise linked. This does not prevent information providers from mirroring or replicating information for performance, security or other mission-related reasons. However, when this is done, the information provider posting the replicated file on its server should contact the content owner of the information and obtain written permission to replicate the information. No copyrighted information may be posted in this process without the permission of the copyright owner. Procedures must also be established for updating the information. In addition, the releasability of the information must be verified by the source from which it is copied. The DoD information provider should continue to control the information to ensure its protection from inappropriate manipulation and make reasonable efforts to verify its currency and accuracy.

2.4. Web Site Registration. All DoD Web sites shall register with the appropriate Service-level site or directly with DefenseLINK.

## 3. INFORMATION POSTING PROCESS

3.1. DoD Component Heads and Heads of subordinate organizations that establish Web sites are responsible for instituting a process for the identification of information appropriate for posting to Web sites and the appropriate security and access controls. The steps of this process (see illustration 1) include:

3.1.1. Identification of information that needs to be conveyed quickly and efficiently and thus will benefit from the attributes of the Web;

3.1.2. Identification of a specific target audience for the information;

3.1.3. Identification of the DoD Originating Office for the information if the sensitivity of the information or distribution restrictions on its release cannot be readily ascertained;

3.1.4. Review of the content for sensitivity and distribution/release controls, including sensitivity of information in the aggregate;

3.1.5. Determination of the appropriate access and security controls;

3.1.6. Approval of the information for public release in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29 (references (h) and (o)) if it is to be posted to a publicly accessible Web site;

3.1.7. Posting the information, once all required steps have been taken;

3.1.8. Verification; and

3.1.9. Feedback reporting, to include “Lessons Learned.”

## INFORMATION POSTING PROCESS

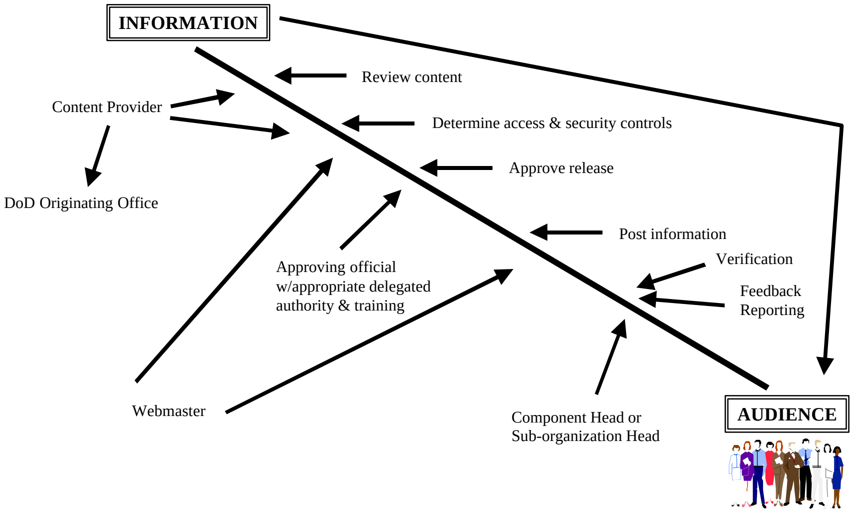


**Illustration 1. Information Posting Process**

3.2 Identification of Information. The World Wide Web provides the DoD with a powerful tool to convey suitable information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies and programs. It is at the heart of the Defense Reform Initiative and is key to the reengineering and streamlining of our business practices. The American democratic process rests on the right of our citizens to know what government is doing, and the corresponding ability to judge its performance. Access to information by the public through the Web is an important component of this right. Nevertheless, careful examination of the potential consequences of placing information on the Web must be undertaken before it is made available.

3.2.1. The identification of a need to post information to a Web site will normally be made by the entity that generates the information and thus has the best knowledge of its content.

3.3. Identification of Target Audience. Illustration 2 depicts many of the target audiences for DoD information posted to the Web. Only information of value to the general public and which does not require additional protection should be posted to publicly accessible sites on the World Wide Web. Information requiring additional protection, such as FOR OFFICIAL USE ONLY (FOUO) information, information not specifically cleared and approved for public release, or information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to the DoD, including military personnel and civilian employees, should be placed on Web sites with security and access controls.

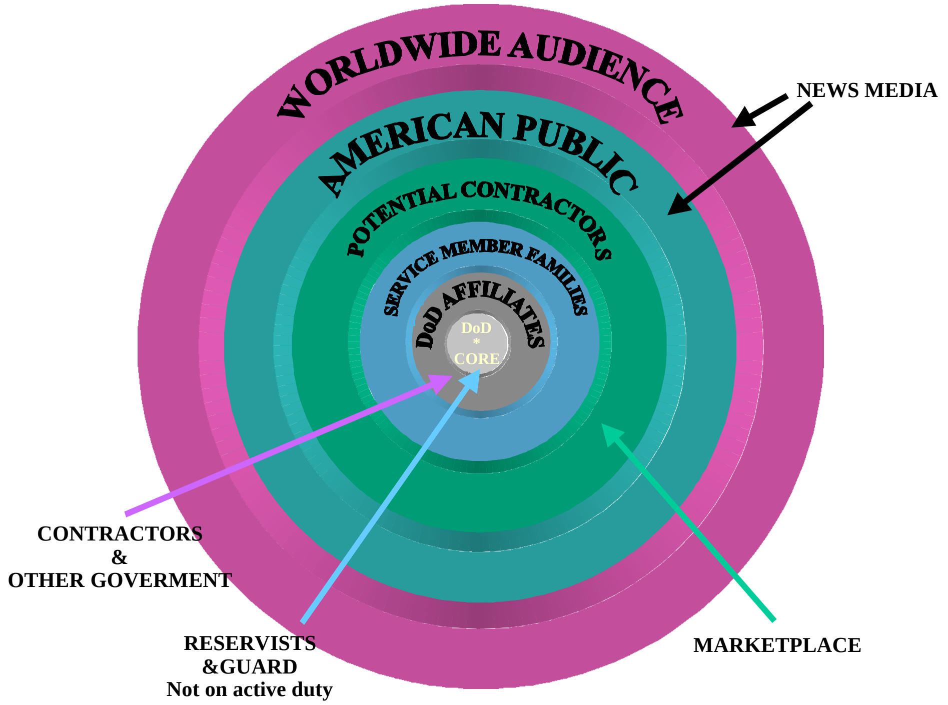


**Illustration 2. Target Audience**

3.4. DoD Originating Office (DOO). Is the entity that created or sponsored the work that generated the information or received/acquired the information on behalf of the DoD. The DOO has the responsibility for assigning appropriate markings to information to include its sensitivity (i.e. classified, FOR OFFICIAL USE ONLY, or other distribution control markings for unclassified information), its releasability to the public, and the approved audience for access (e.g. DoD only, contractors, general public, etc.). The DOO shall be consulted whenever there is doubt with regard to the sensitivity of the information or distribution restrictions on its release.

3.5. Content Review.

3.5.1. Clearance Requirements for Publicly Accessible Web Sites. Heads of DoD Components must establish, in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29 (references (h) and (o)), clearance review procedures for official DoD information that is prepared by or for DoD personnel and is proposed for posting to publicly accessible Web sites.

3.5.2. The above procedures must address the need for trained and knowledgeable personnel, familiar with the rules governing FOR OFFICIAL USE ONLY (FOUO) information as well as pertinent security classification guides, as appropriate. Such individuals must also be familiar with the aspects of the organization's operations considered critical, its vulnerabilities, as well as the pertinent threat in order to assess the nature of the risk associated with posting specific information to Web sites. This risk assessment must also include the increased sensitivity of certain information when electronically aggregated in significant volume.

3.5.2.1. In assessing the increased sensitivity that information may assume in electronic format, it is necessary to take into account the attributes of data mining (i.e., the nontrivial extraction of implicit, previously unknown, and potentially useful information from data). Data mining uses machine learning, statistical and visualization techniques to discover and present knowledge in a form, which is easily comprehensible to humans.

3.5.2.2. The content provider will also take into account the form in which the information was distributed, such as press releases, press conferences, or publicly disseminated documents, the susceptibility of the information to data mining, and the likelihood that the information could directly lead to the discovery and presentment of knowledge that is otherwise controlled (e.g., classified information or FOUO information). Also to be assessed is a specific risk to the Department's credibility if publicly released information is omitted and/or deleted from the Web.

3.5.2.3. If the overall risk resulting from posting the information is determined to be unacceptable, the information must be afforded security and access controls. Part V of this document provides additional guidance in this area while the paragraphs below provide specific prohibitions.

3.5.3. FOR OFFICIAL USE ONLY (FOUO). Information, the disclosure of which would cause a foreseeable harm to an interest protected by one or more of the exemptions to the Freedom of Information Act (FOIA), shall not be posted to a publicly accessible Web site. This information is designated FOUO pursuant to reference (j). While records containing FOUO information will normally be marked at the time of their creation, records that do not bear such markings shall not be assumed to contain no FOUO information without examination for the presence of information that requires continued protection and qualifies as exempt from public release. This may require coordination with the DOO for the information. The following examples are illustrative of the type of information that may be considered to be FOUO. **These examples are not an exclusive listing and they are not intended to offer any guidance in responding to Freedom of Information Act (FOIA) requests.**

3.5.3.1. Analysis and recommendations concerning lessons learned which would reveal sensitive military operations, exercises or vulnerabilities.

3.5.3.2. Reference to unclassified information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of a military plan or program.

3.5.3.3. Personal information including compilations of names of personnel assigned to overseas, sensitive, or routinely deployable units.

3.5.3.4. Information, the release of which would be a clearly unwarranted invasion of personal privacy, to include the following categories about U.S. citizens, DoD employees and military personnel: 1) Social Security Account Numbers;

2) dates of birth; 3) home addresses, and 4) telephone numbers other than duty office numbers. Duty phone numbers of units described in paragraphs C.3.2.1.6.2.2. of DoD 5400.7-R (reference (j)) may not be posted.

3.5.3.5. Names, locations, and specific identifying information about family members of DoD employees and military personnel.

3.5.3.6. Proprietary information submitted by a contractor and protected by a Limited Rights Statement or other agreement, and trade secrets, commercial and financial information submitted by an entity outside the government which considers the information to be protected from release to the public.

3.5.3.7. Test and evaluation information that could result in an unfair advantage or disadvantage to the manufacturer or producer.

3.5.3.8. Technical Information not marked or otherwise determined to be appropriate for Distribution Statement A in accordance with DoD Directive 5230.24 (reference (r)). This includes all technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment.

3.5.4. Unclassified information pertaining to classified programs. The clearance review procedures for unclassified information pertaining to classified programs proposed for posting to a publicly accessible Web sites must take into account the likelihood of classification by compilation. Consultation with the program security classification guide may be required to determine the likelihood that the information, if compiled or aggregated with other information likely to be contained on publicly accessible Web sites, will reveal an additional association or relationship that meets the standards for classification under DoD 5200.1-R (reference (kk)). If such information is posted to a Web site, it must be afforded security and access controls as specified in Part V of this document.

3.5.4.1. In instances where a question arises as to whether information in compilation/aggregation requires protection as classified information, and the information has not yet been entered onto the Web site, the DOO(s) for the information shall be contacted to obtain a decision on the matter before the information is posted. Where the information has already been posted, the information will be withdrawn from the system and will not be re-posted until a decision is obtained from the DOO(s) for the information. In instances where there is a conflict among the DOOs as to the sensitivity of the information, which they are unable to resolve, the matter may be referred to the next higher level within each of the DOOs' organizations until a resolution can be obtained.

3.5.4.2. Users of a Web site who believe that information in compilation or aggregation on a system or systems to which they have access contains classified information, should contact the webmaster of the system(s) in question or, if the webmaster is unknown, report the matter to their own organization's security office for evaluation and action as appropriate.

3.5.4.3. When conducting multi-disciplinary security assessments of Web sites, advanced search engines (e.g. high-end natural-language-based systems optimized for English syntax analysis) and other automated means will be used to assess the likelihood of the presence of information classified by compilation

3.5.5. Copyrighted Material. Copyrighted material will be used only when allowed by prevailing copyright laws and may be used only if the materials relate to the Component’s mission. Consult with Counsel when using any copyrighted material.

3.5.6. Conflicts of Interest. In accordance with the Joint Ethics Regulation (reference (k)), product endorsements or preferential treatment of any private organization or individual shall not appear on any official DoD publicly accessible site.

3.6. Access Controls.

3.6.1. A DoD Web site may not post FOR OFFICIAL USE ONLY information, or information not specifically cleared and approved for public release unless it employs adequate security and access controls. Information of questionable value to the general public must be evaluated before worldwide dissemination to assess the risk to the DoD. Adequate security and access controls must likewise be employed for such information if it is determined to place national security, DoD personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk.

3.6.2 Determinations as to the appropriate security and access controls to employ will be based upon the sensitivity of the information, the target audience for which the information is intended, and the level of risks to DoD interests. Part V of this document contains additional guidance.

3.6.3. Publicly accessible DoD Web sites will not normally contain links or references to DoD Web sites with security and access controls. Under certain circumstances, however, it may be appropriate to establish a link to a log-on site provided details as to the controlled site’s contents are not revealed.

3.7. Release Approval. Approvals for posting of information to publicly accessible Web sites must be in accordance with the provisions of DoD Instruction 5230.29 (reference (o)). Approvals can be granted only by an appropriately trained individual specifically delegated that authority by the Head of the DoD Component or his or her designee.

3.8. Information Posting. Once the procedures established in paragraphs 3.2, 3.3, 3.5, and 3.6. have been completed, the information may be posted to the Web. In addition, the following steps must be accomplished:

3.8.1. A reasonable effort to validate the accuracy of the information.

3.8.2. All links associated with the Web site have been validated.

## 4. ADMINISTRATION AND VERIFICATION

4.1. Web Server Environment Administration. Procedures governing the administration of the Web server environment must be established and, as a minimum, address the following:

4.1.1. Operation of the Web server environment.

4.1.2. Security of the Web server environment.

4.1.3. Maintenance of access and security control features and ensuring that warning and consent to monitoring notices are posted as appropriate.

4.1.4. Ensuring designated approving authority (DAA) approval is re-accomplished if any configuration changes are made to the Web server environment.

4.1.5. Ensuring all links from pages under its control are appropriate and valid.

4.1.6. Establishing procedures for content providers and page maintainers to place information on the Web server.

4.1.7. Granting and monitoring write-access privileges.

4.1.8. Maintaining and evaluating audit control logs.

4.1.9. Gathering and analyzing performance data.

4.1.10. Developing, coordinating, publishing, maintaining, and testing support plans for contingency and service restoration.

4.1.11. Coordinating mirror or replication sites with other system administrators, as required.

4.1.12. Implementing security and access controls requested by content providers and page maintainers as required.

4.1.13. Ensuring access lists are maintained where appropriate.

4.1.14. Incorporating a feedback mechanism for users' comments in accordance with the Paperwork reduction Act of 1995 (reference (a)).

4.2. Verification. Procedures must be established for each DoD Web site to ensure that:

4.2.1. A comprehensive, multi-disciplinary security assessment addressing both content and technical issues is conducted at least annually.

4.2.2. Periodic reviews are conducted to assess compliance with established information posting procedures.

4.2.3. Outdated or superseded information is identified and promptly removed from the system or appropriately archived.

4.3. Feedback Reporting.

4.3.1. Reserve component assets used for DoD-wide OPSEC and threat assessment of unclassified DoD Web sites will observe feedback reporting to include "Lessons Learned."

4.3.2. Web site content providers and administrators will support and participate in the feedback reporting system.

4.3.3. Web site content providers and administrators will review "Lessons Learned" and incorporate content and security changes where appropriate.

5. System Security Considerations

5.1. Operators of DoD Web server environments shall be trained in technical information security best practices, or shall have immediate access to appropriately trained individuals. Security maintenance and administration shall be considered an essential element of Web site operation and maintenance at all times.

5.2. A formal risk assessment shall be conducted at each organization operating a DoD Web site to determine the appropriate risk management approach based on the value of the information; the threat to the DoD Web server environment and the information contained thereon; the vulnerability of the DoD Web server environment and the information contained thereon; and the countermeasures employed by the DoD Web server environment. A security policy shall be written for each DoD Web server environment or multiple sites furnishing similar data on the same system infrastructure or architecture based on the results of the risk assessment.

5.3. DoD Web servers that are externally accessed shall be isolated from the internal network of the sponsoring organization. The isolation may be physical, or it may be implemented by technical means such as an approved firewall. The server software will be FIPS 140-1 compliant with all security patches properly installed. Approved DoD security protocols will be used for all Web servers. Additional security measures shall also be employed consistent with the risk management approach and security policy of the individual DoD Web site. Examples of additional measures to be considered include:

5.3.1. Disable IP forwarding, avoid dual-homed servers

5.3.2. Employ least privilege

5.3.3. Limit functionality of Web server implementation

5.3.4. Employ tools to check configuration of host

5.3.5. Enable and regularly examine event logs

5.4. In addition, all DoD Web servers shall employ a back-up methodology as part of the Web site architecture. Information shall be replicated to the back-up environment to ensure that the information will not be lost in the event that the Web server environment is corrupted, damaged, destroyed or otherwise compromised.

5.5. In cases where an organization operating a DoD Web site determines a requirement to host both a public and non-public Web server, then additional security measures shall be required for the non-public Web server. At minimum, appropriate access controls, audit of security events, and additional measures to ensure confidentiality, integrity and availability of the information shall be employed (see Part V).

5.6. ID and Password Protection. The Internet is an unsecured network where compromise of user ID and password can occur during open transmission. IDs and passwords should not be transmitted without encryption. Secure protocols (e.g. secure sockets layer (SSL) protocol) provides a transmission level of encryption between the client and server machines.

5.7. It is essential that DoD Web server environment be implemented and maintained by certified personnel in accordance with OSD memorandum, subject: Information Assurance (IA) Training and Certification (reference (ll)). Day-to-day maintenance of the hardware and software, including security patches and configurations, is essential to the system security posture of DoD Web server environments.

## 6. GOVERNMENT INFORMATION LOCATOR SERVICE (GILS) REQUIREMENT

DefenseLINK is the central registration point for DoD Web sites. Each Service-level site will establish and maintain registration systems, integrated with DefenseLINK, for their Service. All DoD Web sites shall register with the appropriate Service-level site or directly with DefenseLINK. As part of the registration process, a release authority for the information must be named and the entrant must certify that the content of the Web site complies with the policies set forth in the issuance.

## 7. PRIVACY AND SECURITY NOTICE

A privacy and security notice must be given to users of each Web site and shall be prominently displayed or announced on at least the first page of all major sections of each Web site. Providing a statement such as "Please read this privacy and security notice." linked to the actual notice is satisfactory. Organizations shall avoid flashy graphics or other indicators that create a misperception of danger, such as skull-and-crossbones logos or "warning" signs. If the Web site collects any information on usage or other log files, visitors shall be notified of what information is collected, why it is collected and how it is used. Agencies subject to DoD Directive 5240.1 (reference (q)) must comply with its provisions. The texts of privacy and security notices are provided in Part V of this document.

## 8. EXTERNAL LINKS

8.1. Approval. The ability to hyperlink to sources external to your organization is a fundamental part of the World Wide Web, and can add significant value to the functionality of publicly accessible DoD Web sites. DoD Components must establish objective and supportable criteria or guidelines for the selection and maintenance of links to external Web pages.

8.1.1. Links to non-DoD Web resources should support the organization's mission. External links should be reviewed periodically to ensure their continued suitability. If the content of a linked external site becomes questionable or objectionable, remove the link.

8.1.2. In accordance with DoD 5500.7-R (reference (k)), no product endorsements or preferential treatment shall be given on publicly accessible official DoD Web sites.

8.1.3. No payment of any kind shall be accepted in exchange for a link placed on an organization's publicly accessible official DoD Web site.

8.1.4. In accordance with DoD 5500.7-R, publicly accessible DoD Web sites shall not require or encourage users to choose any specific browser software. Only text or hyperlinked text shall be used to direct visitors to software download sites. Graphics or logos depicting companies/products shall not appear on publicly accessible DoD Web sites.

8.1.5. Organizations considering the use of "frames" technology to connect to external sites should consult legal counsel concerning trademark and copyright issues before establishing such links.

8.1.6. Organizations are encouraged to link to authorized activities in support of the organization's mission, such as the Army and Air Force Exchange Service (AAFES, http://www.aafes.com), the Navy Exchange Service Command (NEXCOM, http://www.navy-nex.com) and the Marine Corps Exchange. If these sites contain commercial advertisements or sponsorships, the appropriate disclaimer below shall be given.

8.1.7. When external links to non-government Web sites are included, the head of the DoD Component, or the subordinate organization, is responsible for ensuring that a disclaimer is made that neither the DoD nor the organization endorses the product or organization at the destination, nor does the DoD exercise any responsibility over the content at the destination. This includes credits given to contractors who produce DoD Web sites.

8.1.8. When a publicly accessible DoD Web site is intended to serve a public purpose, organizations must realize that once the decision is made to include a link to one non-DoD site, the organization may have to link to all similar sites.

8.2. Disclaimer for External Links. The disclaimer below shall be displayed when linking to external sites. This disclaimer may appear on the page or pages listing external links, or through an intermediate "exit notice" page generated by the server machine whenever a request is made for any site other than the official DoD Web site (usually the .mil domain). An example of such an exit notice is located at the White House WWW site at http://www.whitehouse.gov/.

> "The appearance of hyperlinks does not constitute endorsement by the (Department of Defense/the U.S. Army/the U.S. Navy/the U.S. Air Force/the U.S. Marine Corps, etc.) of this Web site or the information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare and Recreation sites, the (Department of Defense/the U.S. Army/the U.S. Navy/the U.S. Air Force/the U.S. Marine Corps, etc.) does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this DoD Web site."

8.3. DoD Newspapers. The policies and procedures in DoD Instruction 5120.4 (reference (n)) apply to all DoD newspapers and civilian enterprise publications, whether printed or electronic. DoD funded newspapers and editorial content of civilian enterprise publications may be posted on DoD Web sites without advertising. Commanders and heads of organizations are authorized to link to a commercial/civilian Web site carrying the authorized civilian enterprise publications, which include advertising, provided the standard disclaimer for external links is given.

## 9. IMAGE MANIPULATION STANDARDS

Official DoD imagery provided on publicly accessible DoD Web sites must conform to DoD Directive 5040.5 (reference (g)).

## 10. COMMERCIAL SPONSORSHIP AND ADVERTISING

Commercial sponsorships, advertisements and endorsements are prohibited on publicly accessible pages of official DoD Web sites. Publicly accessible Web sites are official communications to the public. Just as the DoD would not print advertisements on news releases, the Department shall not post advertisements on publicly accessible official DoD Web sites. Organizations shall ensure that the credibility of official information is not adversely affected by association with commercial sponsorships, advertisements or endorsements.

10.1. Non-appropriated Fund Activities and Web sites. In accordance with DoD Instruction 1015.10 (reference (m)). Morale, Welfare and Recreation (MWR) programs may have commercial sponsors and may sell electronic advertising as outlined in that instruction. As the instruction points out, MWR products with advertisements are intended for distribution to the DoD internal audience authorized to take advantage of these programs.

10.1.1. However, having advertisements on pages that are part of an official, publicly accessible DoD Web site is inappropriate. Organizations are encouraged to include official information about non-appropriated fund (NAF) activities on official DoD Web sites as long as the information does not include commercial sponsorships or advertisements.

10.1.2. With organization approval, NAF activities may use non-appropriated funds to develop and maintain commercial Web sites for unofficial information, where commercial sponsorship or advertising may appear. External links to authorized, unofficial NAF commercial Web sites are authorized, with an appropriate disclaimer preceding the actual connection to the NAF commercial Web site to avoid product endorsement or preferential treatment.

10.1.3. Official information pertaining to the NAF activity may be posted on the commercial non-appropriated fund Web site with installation commander/organization head approval, but only if it is also posted on the official publicly accessible DoD Web site. Other official information shall not be posted to the commercial site.

## 11. DESIGN STANDARDS AND NON-STANDARD FEATURES

11.1. Web site documents shall conform to the approved technical specifications approved in the Joint Technical Architecture (JTA). In situations where World Wide Web Consortium (W3C) recommendations or proposed recommendations are more recent than those examined by the JTA, developers may use the W3C recommendations or proposed recommendations.

11.2. Incorporation of non-standard or browser-specific features into Web pages shall also be evaluated in light of the potential security risks and interoperability. Certain features have the capability of installing malicious programs on networks or on individual machines, if downloaded. The same danger exists when downloading any executable file, which is why many organizations have a policy in place prohibiting downloads of such files. In general terms, it is recommended that existing local guidelines concerning the download/installation of executable files should apply to any software that installs programs on networks or individual machines. Use of non-standard or browser specific features may exclude a portion of a Web site's audience, and should be avoided.

## 12. COLLECTION OF INFORMATION

To better serve the public, in certain instances it is necessary and appropriate to collect information from visitors to Web sites.

12.1. Survey Forms/Information Collections.

12.1.1. In accordance with the Paperwork Reduction Act of 1995, (PRA), (reference (a)), collection of information from the public shall be approved by OMB under some circumstances.

12.1.2. Requests for identical information from ten or more members of the public must be approved by OMB, such as surveys using check box, radio button or text form fields.

12.1.3. The PRA applies to electronic forms/information collections on Web sites that collect standardized information from the public. It does not apply to collection of information strictly from current DoD employees or service members in the scope of their employment. Surveys on publicly accessible Web sites will not ordinarily be exempt from the requirement to obtain OMB approval under this exception.

12.1.4. Forms for general solicitations of comments that do not seek responses to standard questions, such as the common opinion-based feedback forms and e-mail links, do not require OMB clearance.

12.1.5. Organizations are responsible for ensuring their publicly accessible Web sites comply with this requirement and follow procedures in DoD 8910.1-M (reference (l)). For more information about the Paperwork Reduction Act of 1995, contact your local Information Management Control Office.

12.2. Usage Statistics. As a management function, evaluation of site usage data (log files) is a valuable way to evaluate the effectiveness of Web sites. However, collection of data from publicly accessible sites for undisclosed purposes is inappropriate. There are commercially available software packages that will summarize log file data into usable statistics for management purposes, such as the most/least requested documents, type of browser software used to access the Web site, etc. Use of this type of software is appropriate, as long as there is full disclosure as specified in the privacy and security notice, referenced above. Organizations shall establish a destruction disposition schedule for collected data.

12.3. User-identifying Collection Methods for Public Web Sites. In accordance with the privacy and security notice referenced above, it is prohibited to use methods which collect user-identifying information such as extensive lists of previously visited sites, e-mail addresses, or other information to identify or build profiles on individual visitors to publicly accessible Web sites. It is permissible to use "cookies" or other methods to collect or store non-user-identifying information; however, users shall always be notified of what information is collected or stored, why it is being done and how it is used. Agencies subject to DoD Directive 5240.1 (reference (q)) must comply with its provisions.

## 13. DoD WEBMASTER LISTSERV

To share and coordinate information, an e-mail listserv has been established for all DoD "Webmasters." All personnel responsible for developing and/or maintaining a Web site are encouraged to join this listserv. Although an Army unit maintains it, the list is open to members in all services. Instructions are located at “http://www.army.mil/Weblist.htm”

14. EFFECTIVE DATE: These procedures are effective 120 days from the date of this document.

# WEB SITE ADMINISTRATION

## Part III – Definitions

November 25, 1998

**DefenseLINK**. The name of the official publicly accessible Web site for the Department of Defense (DoD). DefenseLINK provides the official single point of access to all DoD information on the World Wide Web, and establishes a means to ensure that the information is readily accessible, properly cleared and released, accurate, consistent, appropriate and timely.

**DoD Originating Office (DOO).** Is the entity that created or sponsored the work that generated the information or received/acquired the information on behalf of the DoD.

**Home page**. The index or introductory document for a Web site.

**Internet**. The loosely connected worldwide collection of computer systems that uses a common set of communications standards to send and receive electronic information.

**Operations Security (OPSEC).** OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to defense acquisitions, military operations, and other activities in order to: i) identify those actions that can be observed by adversary intelligence systems; and ii) determine what indicators might be obtained by hostile intelligence systems that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and iii) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation

**Official DoD Web site**. A DoD Web site that is developed and maintained with command sponsorship and approval, and for which the DoD Component, a subordinate organization or individual, exercises editorial control over content. The content of official DoD Web sites is of an official nature that may be endorsed as the official position of the DoD Component. Content may include official news releases, installation history, command position papers, etc. Official DoD Web sites are prohibited from displaying sponsorships or commercial advertisements.

**Technical Information**. Information, including scientific information, which relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment. (JCS Pub 1)

**Unofficial DoD Web site**. A DoD Web site that is developed and maintained with non-appropriated funds; and for which the DoD Component, or a subordinate organization, does not usually exercise editorial control over content. The content of unofficial DoD Web sites is not endorsed as the official position of the DoD Component. Content will not normally include official news releases, installation history, command position papers, etc. Unofficial DoD Web sites may include sponsorships and commercial advertisements, and may also advertise products for sale, in accordance with the mission of the organization. In most cases, unofficial DoD Web sites are developed and maintained by commercial or nonprofit organizations. Certain military-affiliated organizations may develop and maintain unofficial DoD Web sites. Such organizations include service exchanges and Morale, Welfare and Recreation activities that use non-appropriated funds.

**World Wide Web or Web**. The subset of the Internet capable of providing the public with user-friendly graphics-based multi-media access to information on the Internet. It is the most popular means for storing and linking Internet-based information in all multi-media formats. Navigation is accomplished through a set of linked documents that may reside on the same computer or on computers located almost anywhere else in the world.

**Web site**. A collection of information organized into a number of Web documents related to a common subject or set of subjects, including the "home page" and the linked subordinate information.

**Web Server Environment** The physical computing resources, including servers, software, network, communications, security, and peripheral devices that provide the platform upon which Web sites are made available to users through internetworking.

# WEB SITE ADMINISTRATION

## Part IV – References

November 25, 1998

(a) 44 USC Chapter 35, "Paperwork Reduction Act", as amended

(b) Government Printing and Binding Regulations, Joint Committee on Printing, Congress, US, February 1990, No. 26

(c) National Archives and Records Administration General Schedule 20, August 1995

(d) Deputy Secretary of Defense Policy Memorandum, "Government Information Locator Service (GILS)," September 2, 1995

(e) Chairman, Joint Committee on Printing Memorandum granting waiver for Commercial Enterprise Newspapers, July 15, 1983

(f) Office of Management and Budget (OMB) Bulletin 95-01, "Establishment of Government Information Locator Service," December 7, 1994

(g) DoD Directive 5040.5, "Alteration of Official DoD Imagery," August 29, 1995

(h) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996

(i) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 22, 1997

(j) DoD 5400.7-R, "DoD Freedom of Information Program Regulation", September 1998

(k) DoD 5500.7-R, Joint Ethics Regulation (JER), August 30, 1993

(l) DoD Directive 8910.1-M, "DoD Procedures for Management of Information Requirements," June 11, 1993

(m) DoD Instruction 1015.10, "Programs for Morale, Welfare, and Recreation (MWR)," November 3, 1995, w/ Ch 1, October 31, 1996

(n) DoD Instruction 5120.4, "DoD Newspapers and Civilian Enterprise Publications," June 16, 1997

(o) DoD Instruction 5230.29, Security and Policy Review of DoD Information for Public Release," May 6, 1996

(p) AR 60-20/AFR 147-14, "Army and Air Force Exchange Service Operating Policies," 15 December 1992

(q) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988

(r) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987

(s) DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984

(t) Public Law 100-235, "Computer Security Act of l987"

(u) DoD Directive 5200.5, "Communications Security (COMSEC)," April 21, 1990

(v) DoD Directive 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997

(w) DoD Directive 4640.6, "Communications Security (COMSEC) Telephone Monitoring and Recording, " June 26, 1981

(x) DoD Directive 5205.2, "DoD Operations Security Program," July 7, 1983

(y) DoD Instruction 3200.14, "Principles And Operational Parameters of the DoD Scientific and Technical Information Program," May 13, 1997, Enl 6

(z) International Traffic in Arms Regulation (ITAR), Department of State, May 1998

(aa) Wassenaar Arrangement, see Federal Register, January 15, 1998 (Vol 63 No. 10) pages 2451 – 2500

(bb) Carnegie Mellon University Software Engineering Institute, “Security for a Public Web Site,” CMU/SEI-SIM-002, August 1997

(cc) National Institute of Standards and Technology (NIST), “Internet Security Policy: Technical Guide,” http://csrc.nist.gov/isptg/html/ISPTG-Contents.html

(dd) Defense Information Systems Agency (DISA), “DISA/NCS World Wide Web (WWW) Handbook Version 2.2,” http://www.disa.mil/handbook/toc.html

(ee) DoD Directive 8500.xx, "Information Assurance," draft

(ff) DoD Instruction 8500.xx, "Information Assurance Requirements," draft

(gg) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, "National Information Systems Security Glossary," August 1997.

(hh) DoD General Counsel Memorandum, "Communication Security and Information Systems Monitoring," March 17, 1997

(ii) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988

(jj) DoD 5025.1-M, "DoD Directive Systems Procedures, August 1994

(kk) DoD 5200.1-R, "Information Security Program, " January 1997

(ll) USD (P&R) and OASD (C3I) memorandum entitled "Information Assurance (IA) Training and Certification," June 29, 1998.

# WEB SITE ADMINISTRATION

## Part V – Examples & Best Practices

November 25, 1998

1.. INFORMATION VULNERABILITY, THE WEB AND OPSEC

1.1. General

1.1.1. Over the last three decades, the world has experienced the rapid integration of information processes and telecommunications technology. As we leveraged these gains, the national security posture of the United States has become increasingly dependent on the Defense (DII), National (NII) and the larger Global Information Infrastructure (GII). These information infrastructures (which consist of information, information systems, telecommunications, networks, and technology) represent lucrative targets in an increasingly asymmetrical threat environment.

1.1.2. Within this global infrastructure lies a mosaic of interconnectivity which is growing at a rate of 500,000 new World Wide Web (WWW) entry points a month. This interconnectivity, when coupled with search engines and information compilation algorithms, provides a single user the ability to aggregate, analyze, and construct new levels of understanding from unclassified sources. As such, the information provided on publicly accessible Web sites is an OPSEC concern.

1.1.3. This section addresses why information technology makes sensitive but unclassified information vulnerable. It will address why certain types of DoD information cannot be posted to publicly accessible Web sites within the context of the OPSEC process.

1.2. Information Technology

1.2.1. The information infrastructure is extremely complex. There is no simple way to define and establish its bounds, to measure its impact, or to identify clear responsibilities for its evolution, operation, maintenance, and repair. Therefore, the various views of the infrastructure presented here only partially address the complexity.

1.2.2. One way of viewing the information infrastructure is in terms of its basic components. In simple terms, the information infrastructure is comprised of the components necessary for the transportation of information, the information itself, the means for creating, gathering, and processing data to obtain information, and the storage of the data and information.

1.2.3. Another way of viewing the information infrastructure is as a collection of networks and services. Some of these networks and services, such as the Internet and public telephone and data networks, have an identity of their own and are clearly an integral part of the Information infrastructure. Others, such as financial networks and services, have developed within a specific industry and evolved into a complex inter-network necessary to provide responsive support to the customer. This is particularly true regarding the Defense Information Infrastructure (DII).

1.2.4. The information infrastructure can also be thought of in terms of the various domains it serves. These infrastructure domains have the potential of containing vast amounts of sensitive but unclassified information. This has not gone unnoticed by Internet users who have developed and are now refining sophisticated “data mining” tools and techniques that allow precision targeting and rapid aggregation of data.

1.2.5. When you combine these infrastructure components, networks and services, and domains, the OPSEC oriented user will quickly recognize the vast resources of information available to the public and the adversary. The potential for inadvertent or unauthorized disclosure of sensitive information continues to grow.

1.3. Information Vulnerability and the OPSEC Process

1.3.1. Given the increasing dependence of our national and economic security upon the information infrastructure, it is essential that the commander and other organizational Heads review organizational information connectivity and content to ensure good OPSEC procedures are being applied within their organizations. As such, risk assessment and risk management become critical factors in evaluating publicly accessible Web site information.

1.3.2. The worldwide connection of computer local area networks (LAN) and wide area networks (WAN) such as the NIPRNET makes access to defense information from anywhere in the world relatively easy. Separation between the NIPRNET and the WWW is ambiguous, and occasionally these networks may be indistinguishable to Web page administrators. Web pages intended for internal DoD use should not be made available on the NIPRNET without appropriate access control, as this information is likely to be accessible to non-DoD users. Consequently, OPSEC and INFOSEC concerns arise.

1.3.3. This requires a convergence of Information Security (COMPUSEC and COMSEC) tools and the OPSEC process at the activity level. Activity webmasters, page maintainers, subject matter experts and OPSEC personnel must develop a disciplined review of all information posted to their locally generated Web sites. This must be done to protect sensitive unclassified and classified information -- while recognizing the importance of making available timely and accurate information to the intended DoD audiences, the public, Congress, and the news media.

1.3.4. Evaluations of activity information provided on the NIPRNET and publicly accessible DoD Web sites on the Internet should follow current OPSEC methodology:

1.3.4.1. Identify information access points (NIPRNET, Internet, etc.,..) and evaluate their importance to activity operations.

1.3.4.2. Determine the critical information for the activity's operations and plans. Information that would not be of interest/use to the general public should not be on a public access page.

1.3.4.3. Determine the threat –assume that any potential adversary has access and knows how to search the net.

1.3.4.5. Determine the vulnerabilities – how protected are the Web pages? Remember, the hacker is generally the INFOSEC threat, the search engine and browser are generally the OPSEC threat.

1.3.4.6. Assess the risk – what protection should be applied to minimize potential loss of critical information and what is the impact on operations and operations support?

1.3.4.7. Apply protection – combine INFOSEC and OPSEC tools to minimize information loss and vulnerability.

1.3.5. When applying the OPSEC process to information posted to Web sites, the activity will also need to evaluate subject data with regard to the time factor. Information gathering in the past was a manpower and resource intensive process that was dependent on various types of overt and clandestine means. Collection, compilation, analysis, and dissemination of information could take days, weeks, or months. Today, a single user can connect to the Web and using varying search engines, browsers, and certain aggregation methods develop a composite of information that surpasses traditional knowledge levels. In essence, geography is no longer a factor in information retrieval--time becomes the dominant factor.

1.3.6. As such, the user must determine the value of information with regards to time. Certain data such as unit history, emblems, command affiliation, etc. will have less time criticality than will deployment orders for exercises or real world operations. The value of information may also flex over time. For example, the specifics of post-deployment preparations should not be posted to a publicly accessible Web site prior to the deployment. But once in theater, unit types, number of personnel and equipment will become public knowledge over time, decreasing the sensitivity of the data. Subsequently, the same information will again become sensitive as redeployment dates and unit withdrawal specifics are planned. This will require units to actively scrub their Web pages for time sensitive data.

1.4. Conclusion. Operations security is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other sensitive activities. OPSEC training and education apply to computer use just as it does in conversations between personnel, correspondence, and telephone conversations. In the past, OPSEC has focused on activities that might be seen by a human observer, a satellite, a radio intercept operator or the news. But with the proliferation of information technologies over the last three decades, the access to DoD data has grown exponentially. The old threats have not gone away, but there is a new area of concern that OPSEC officers and planners must consider – the Internet. A disciplined approach to INFOSEC procedures in conjunction with the OPSEC process will ensure that sensitive but unclassified information is properly safeguarded.

## 2. GUIDE FOR IDENTIFYING INFORMATION INAPPROPRIATE FOR POSTING TO A PUBLICLY ACCESSIBLE DOD WEB SITE

This guidance is authorized to be used for one purpose only: identifying information that may be inappropriate for posting to publicly accessible DoD Web sites. **It is not to be used as guidance in responding to requests under the FOIA or the Privacy Act under any circumstances.** It is intended as an interim guide to the identification of categories of information that are inappropriate for posting to a publicly accessible Web site. Additional guidance will be forthcoming when this document is formalized in the DoD publication system.

FOR OFFICIAL USE ONLY (FOUO) information may not be posed to official Web sites that are open to public access. (Information which is typically FOUO is followed by an * below). Also identified below is information whose sensitivity may be increased when electronically aggregated in significant volume. All information proposed for posting to a publicly accessible Web site must be reviewed in accordance with the provisions of DoD Directive 5230.9 and DoD Instruction 5230.29 (references (h) and (o)) and as described in Paragraph 3, Part II of this document.

Do not use this compendium as the sole source for identifying such information. Questions about FOUO information should be referred to your local FOIA office. Questions about aggregated information should be referred to your local security office and/or OPSEC coordinator.

2.1 Military Operations & Exercises information relating to:

- Unit Organization
- Unit readiness specificity
- Detailed mission statement
- Specific Unit phone/fax numbers (secure and unsecured)
- Time-Phase Force Deployment Data (TPFDD)
- Ops schedules
- Logistics support requirements
  - Medical
  - Civil engineering
  - POL
  - Host nation support
  - Transportation
  - Munitions
- Force Apportionment
- Force Allocation
- Unit Beddown information
- Planning guidance
- Unit augmentation
- Force Synchronization
  - Unit shortfalls
- Counter-terrorism information
- Detailed Budget Reports
- Images of Command and Control (C2) nodes
- Inventory reports
- Intelligence, Surveillance and Reconnaissance (ISR) Capabilities
- Command, Control, Communications, Computers and Intelligence(C4I) Architecture
- Non-Combatant Evacuation Operations (NEO) Plans or Ops
- Counter-drugs Ops
- Unit Recall Rosters
- Weapons Movements
- Mobilization information
- Detailed maps or installation photography
- Standard Operating Procedures
- Tactics, Techniques, and Procedures
- Critical maintenance

2.2. Personnel information relating to:

- Information, the release of which would be a clearly unwarranted invasion of personal privacy, to include the following categories about U.S. citizens, DoD employees and military personnel: (1) Social Security Account Numbers; 2) dates of birth; 3) home addresses, and 4) telephone numbers other than duty office numbers. Duty phone numbers of units described in C.3.2.1.6.2.2. of DoD 5400.7-R (reference (j)) may not be posted.*

- Names, locations, and any other identifying information about family members of DoD employees and military personnel*
- Official travel itineraries of individuals and units before it is performed*
- Duty rosters, or detailed organizational charts and directories with names (as opposed to organizational charts, directories, general telephone numbers for commonly requested resources, services and contacts without names)*
- Internal DoD personnel rules and practices unless cleared for release to the public*
- Financial Disclosure Reports of Special Government Employees (5 USC App. 4, §207 (a) (1) 2)*
- Representation Rights and Duties, Labor Unions (5 USC §7114 (b)(4))*
- Action on reports of Selection Boards (10 USC §618)*
- Confidential Medical Records (10 USC §1102)*
- Civil Service Examination (18 USC §1917)*
- Drug Abuse Prevention/Rehabilitation Records (21 USC §1175)*
- Confidential of Patient Records (42 USC §290dd-2)*
- Information Concerning US Personnel Classified as POW/MIA During Vietnam Conflict (42 USC §401)*
- Information Identifying Employees of DIA, NRO, and NIMA (10 USC §424)*

2.3. Proprietary Information submitted by a contractor and protected by a Limited Rights Statement or other agreement, and trade secrets, commercial and financial information submitted by an entity outside the government that considers the information to be protected from release to the public. Other specific provisions include:

- Contractor Proposals (10 USC §2305 (g))*
- Commercial or financial information received in confidence with loans, bids, contracts or proposals*
- Information received in confidence e.g. trade secrets, inventions, discoveries or other proprietary data*
- Statistical data and commercial or financial information concerning contract performance, income, profits, losses and expenditures, if offered and received in confidence from a contractor or potential contractor*
- Scientific and manufacturing processes or developments concerning technical or scientific data and other information submitted with an application for research grant or with a report while research is in progress*
- Test and evaluation of commercial products or military hardware produced by a non-governmental entity*
- Patents, unless licensed for publication by the United States*
- Software documentation: shall be distributed according to the terms of the software license*

- Premature Dissemination: The information related to patentable military systems or processes in the developmental stage.*
    - Confidential Status of Patent Applications (35 USC §122)*
    - Secrecy of Certain Inventions and Withholding of Patents (35 USC §181-188)*
    - Confidential Inventions Information (35 USC §205)*

2.4. Test and Evaluation information could result in an unfair advantage or disadvantage to the manufacturer or producer or could reveal the capabilities, limitations, or incapabilities of a DoD weapons systems or component.

2.5. Scientific and technological information relating to:

- Critical technology on either the Munitions List or the Commerce Control List*
- Unclassified Special Nuclear Weapons Information (10 USC §128)*
- Unclassified Technical Data with Military or Space Application (10 USC §130)*
- Centers for Industrial Technology – Reports of Technology Innovations (15 USC §3705 (e)(E))*
- Information Regarding Atomic Energy (42 USC §2161-2168)*
- Control of Arms Exports Sec 38(e) of the Arms Export Control Act (22 USC §2778(e))*
- Technical and scientific data developed by a contractor or sub-contractor exclusively or in part at private expense*
- Sensitive S&T Reports such as:*
    - Defense Acquisition Executive System Reports
    - Selected Acquisition Reports
    - Weapons System Unit Cost Reports
    - Approved Program Baselines for ACAT I, II, III Weapons Systems
    - Weapons Systems Evaluation and Testing Results and Reports
    - Reports Based on Joint USA and Foreign Government Technical Research and Weapons Systems Evaluations
    - Weapons System Contractor Performance Reporting Under earned Value Reporting System at the Level of CPE Reporting
    - Weapons Systems staff working papers, correspondence and staff assessments
    - DoD Component “Feedback” staff working papers and assessments on weapons System Program Performance

2.6. Intelligence information relating to:

- Organizational & Personnel Information for DIA, NRO and NIMA (10 USC §424)*
- Maps, Charts, and Geodetic Data (10 USC §455)*
- Communications Intelligence (18 USC §798)*
- NSA Functions and Information (50 USC §402)*

- Protection of Identities of US Undercover Intelligence Officers, Agents, Informants and Sources (50 USC §421)*
- Protection of Intelligence Sources and Methods 50 USC §403(d)(3))*

2.7. Other information relating to:

- A-76 studies and other outsourcing studies that provide detailed descriptions of sensitive organizational operations
- Administrative Dispute Resolutions (5 USC §574 (j))*
- Confidentiality of Financial records (12 USC §3403)*
- National Historic Preservation (16 USC §470w-3)*
- Internal advice, recommendations and subjective evaluations*

## 3. SECURITY AND ACCESS CONTROLS

3.1. Determinations as to the appropriate security and access controls to employ will be based upon the sensitivity of the information and the target audience for which it is intended. The table below provides additional guidance to include the vulnerability of various combinations of each. Use this table in conjunction with the above list of types of sensitive information to determine an acceptable level of risk. Do not regard these guidelines as the only options available for protecting information content.

| **If access control is:** | **and transmission control is:** | **the vulnerability is:** | **and the information posted can be:** |
|---|---|---|---|
| Open – Includes Webmaster training and certification, isolation of the server, current version of server software and O/S, with all security patches properly installed | Plain text, unencrypted | Extremely High -- Subject to worldwide dissemination and access by everyone on Internet | Non-sensitive, of general interest to the public, cleared and authorized for public release for which worldwide dissemination poses limited risk for DoD or DoD personnel, even if aggregated with other information reasonably expected to be in public domain. |
| Limited by Internet Domain (e.g. .mil, .gov) or IP address | Plain text, unencrypted | Very High -- Can circumvent access controls, affords lowest level of access control, and no encryption | Non-sensitive, not of general interest to the public although approved and authorized for public release, and intended for DoD or other specifically targeted audience. |
| Limited By User ID and password (e.g. DMDC database or other registration system) | Plain text, unencrypted | High -- Can circumvent access controls, affords higher level of access controls, however, IDs and passwords can be compromised if encryption is not used. | Non-sensitive but limited to a specific, targeted audience. |
| User Certificate Based (Software) Requires PKI | Encrypted text through use of secure sockets layer | Moderate -- Provides moderate level of access controls | FOR OFFICIAL USE ONLY and information sensitive by aggregation |
| User Certificate Based (Hardware) Requires PKI | Encrypted text | Very Low | FOR OFFICIAL USE ONLY and information sensitive by aggregation where extra security is required due to compilation |

**Table 1. Security and Access Controls**

3.2. Until such time as specific technical policy guidelines are formalized for all Internet services , Webmasters and users are encouraged to consult existing authoritative literature on security and access controls. Examples of such literature include, but are not limited to:

3.2.1. Carnegie Mellon University Software Engineering Institute, “Security for a Public Web Site,” CMU/SEI-SIM-002, August 1997.

3.2.2. National Institute of Standards and Technology (NIST), “Internet Security Policy: A Technical Guide,” http://csrc.nist.gov/isptg/html/ISPTG-Contents.html

3.2.3. Defense Information Systems Agency (DISA), “DISA/NCS World Wide Web (WWW) Handbook Version 2.2,” “http://www.disa.mil/handbook/toc.html"

## 4. <u>TEXT OF PRIVACY AND SECURITY NOTICE</u>

4.1. The following privacy and security notice may be tailored in the indicated areas by each organization sponsoring a publicly accessible Web site. The notice shall be approved by the appropriate local legal authority before use.

Link from Index.html pages -- "<u>Please read this privacy and security notice.</u>"

( ) - indicates sections to be tailored at the installation level

[ ] - indicates hyperlinks

* - indicates information located at the hyperlink destination indicated

***Quote:***

### PRIVACY AND SECURITY NOTICE

1. (DefenseLINK) is provided as a public service by the ([Office of the Assistant Secretary of Defense-Public Affairs] and the [Defense Technical Information Center]).

2. Information presented on (DefenseLINK) is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

3. For site management, [information is collected]* for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with [National Archives and Records Administration Guidelines].

*Agencies subject to DoD Directive 5240.1 shall add the following to paragraph 5:* "All data collection activities are in strict accordance with DoD Directive 5240.1 (reference (p))."

6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.

7. If you have any questions or comments about the information presented here, please forward them to (us using the DefenseLINK [Comment Form]
______________________________________________ ***End Quote:***

* Link from above - "information is collected" to the following text:

NOTE: The information below should be tailored, if necessary, to show an accurate example of the specific information being collected.

**Example: Information Collected from (DefenseLINK) for Statistical Purposes**

Below is an example of the information collected based on a standard request for a World Wide Web document:

```
xxx.yyy.com - - [28/Jan/1997:00:00:01 -0500] "GET
/DefenseLINK/news/nr012797.html HTTP/1.0" 200 16704
Mozilla 3.0/www.altavista.digital.com
```

**xxx.yyy.com (or 123.123.23.12)--** this is the host name (or IP address) associated with the requester (you as the visitor). In this case, (....**com**) the requester is coming from a commercial address. Depending on the requester’s method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via many Internet Service Providers assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) will identify a specific computer if that computer has a fixed IP address.

**[28/Jan/1997:00:00:01 -0500]** -- this is the date and time of the request

**"GET /DefenseLINK/news/nr012797.html HTTP/1.0"** -- this is the location of the requested file on (DefenseLINK)

**200** -- this is the status code - 200 is OK - the request was filled

**16704** -- this is the size of the requested file in bytes

> **Mozilla 3.0** -- this identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages
>
> **www.altavista.digital.com** - this indicates the last site the person visited, which indicates how people find (DefenseLINK)
>
> Requests for other types of documents use similar information. No other user-identifying information is collected.

4.2. The following notice and consent banner, approved by the DoD General Counsel (reference (hh)), may be used on all DoD Web sites with security and access controls. This banner may be tailored by an organization but such modifications shall be accomplished in compliance with reference (hh), and shall be approved by the Component's General Counsel before use.

> "This is a Department of Defense Computer System. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.
>
> Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes."

SECNAVINST 5720.47
CHINFO
1 July 1999

SECNAV INSTRUCTION 5720.47

From: Secretary of the Navy
To: All Ships and Stations

Subj: DEPARTMENT OF THE NAVY POLICY FOR CONTENT OF PUBLICLY ACCESSIBLE WORLD WIDE WEB SITES

Ref: (a) DoD Policy Memorandum “Web Site Administration,” Dec 7, 98 (NOTAL)
(b) SECNAVINST 5720.44A, “Department of the Navy Public Affairs Policy and Regulations”
(c) SECNAVINST 5430.97, “Assignment of Public Affairs Responsibilities in the Department of the Navy”
(d) SECNAVINST 5211 .5D, “Department of the Navy Privacy Act (PA) Program”
(e) SECNAVINST 5720.42F, “Department of the Navy Freedom of Information Act (FOIA) Program”
(f) OPNAVINST 5510.36, “Department of the Navy (DON) Information Security Program Regulation”
(g) SECNAVINST 5239.3 “Department of the Navy Information Security (INFOSEC) Program” (NOTAL)
(h) DoD Directive 5040.5 “Alteration of Official DoD Imagery”, Aug 29, 95 (NOTAL)

Encl: (1) DON Web Site Administration Definitions
(2) DON Publicly Accessible Web Site Policy and Procedures

1. Purpose. To implement reference (a) within the Department of the Navy (DON) and provide additional policies and procedures governing the content of Department of the Navy publicly accessible World Wide Web (WWW) sites.

2. Cancellation. ALNAV 084/98, Department of the Navy World Wide Web Policy and ALMAR 3 88/97, Marine Corps World Wide Web Policy.

3. Scope. This instruction is applicable throughout the DON. It applies to all DON activities and all publicly accessible DON Web sites designed, developed, procured, or managed by DON activities and by their contractors.

4. Background

a. The Department of Defense (DoD) has established policy and assigned responsibilities related to establishing, operating, and maintaining unclassified military sites on the World Wide Web (WWW). The World Wide Web is an extremely powerful public information tool, and its use, within the guidelines here, is encouraged. This instruction assigns responsibilities and prescribes policies implementing reference (a) within the DON, to ensure appropriate use of the WWW to provide public information to a global audience.

b. The development of Web browsers and the ease with which documents may be created has given rise to the proliferation of command sites on the World Wide Web. The World Wide Web is, and was specifically designed to be, open and accessible to a global audience. While this global accessibility makes the Web a powerful public information tool, as well as being a productivity enhancer for all commands and staffs in the conduct of daily business, it also can present a danger to DON personnel, assets and operations if inappropriate information is published on command Web sites. The global reach of the World Wide Web requires special precautions be taken when posting information to this medium. Millions of Web users around the world can easily gain access to Navy public Web sites, rapidly collect information, add it to information already collected from other public sites, and assemble it in a way that is not possible through any other form of media. Recent advances in computer software and Internet-based search engines have given Web users the ability to automatically “mine” data and collect an aggregate of information that can pose a threat to the security of Navy operations and the personal safety of Navy forces and their families. More than ever, the need to provide public information to the Navy’s various audiences must be balanced with the need to protect operational security, privacy of information, and personal safety.

c. As the World Wide Web proves itself to be a cost-effective method of moving information and as DON becomes increasingly dependent on the Internet, any sustained attack on the Internet could have serious ramifications. Computer network attacks often begin by gleaning information about a command from its publicly-accessible Web site and combining it with other publicly-accessible information. Additionally, this information may be used by an adversary to disrupt DON operations or target individuals. By its very nature, the World Wide Web greatly facilitates information collection and aggregation.

d. The appearance, accuracy, currency and relevance of the information presented by Navy and Marine Corps commands on their Web sites reflects on the DON’s professional standards and credibility. Additionally, information residing on a Web server associated with a domain is interpreted by the worldwide public, including the American taxpayer and media, as reflecting official DON policies or positions.

e. The benefits of using the World Wide Web as a public information tool must be balanced with security and safety concerns. Commanders must strike a balance between openness in government (easy access to DON information) and the need to safeguard information which, if released to the general, global public, could adversely affect the national interest, the conduct of DON operations and programs, or place DON commands, personnel or their families at risk. Potential risks must be judged and weighed against potential benefits prior to posting any DON information to the World Wide Web.

5. Definitions. Terms used in this instruction are defined in reference (a) and further in enclosure (1).

6. Policy. Reference (a) provides primary governing policy for all unclassified World Wide Web sites. Detailed policy on administration of publicly accessible World Wide Web sites, in amplification of reference (a), is provided in enclosure (2).

7. Action

a. The Department of the Navy Chief Information Officer (DONCIO) is responsible for providing Department wide Information Management and Information Technology (IM/IT) leadership and guidance.

b. The Department of the Navy Chief of Information (CHINFO) and U.S. Marine Corps Director of Public Affairs (DIRPA) are responsible for the development and administration of DON and Marine Corps public affairs policies and procedures respectively per references (b) and (c). Additionally, CHINFO and DIRPA each will:

(1) Maintain master WWW pages to issue new service-specific guidance in response to security/technological or other factors associated with the rapid pace of change in IM/IT. CHINFO will maintain a master WWW page to issue DON guidance and DIRPA will link to that page. All significant changes to this Web page and/or its location will be issued via Naval (ALNAV) message.

(2) Establish and maintain central Web site registration systems for all U.S. Navy or Marine Corps commands as appropriate in accordance with reference (a).

(3) Administer and maintain the official U.S. Navy Web site at www.navy.mil or the official U.S. Marine Corps Web site at www.usmc.mil for the posting of appropriate U.S. Navy- or Marine Corps-level information and images.

(4) Maintain overall cognizance for U.S. Navy Web site or U.S. Marine Corps Web site content-related questions as they pertain to the appropriateness of publicly accessible

material. This responsibility includes cognizance regarding Privacy Act (PA), Freedom of Information Act (FOIA) and public affairs material but will not include issues related to the security of operations or classified information.

(a) For Navy PA/FOIA issues, CHINFO will coordinate, as appropriate, with Office of the Judge Advocate General (OJAG) (Code 13) and/or the Chief of Naval Operations (CNO)(N09B3 0). CNO (N6) is responsible for issues related to security of operations and classified information.

(b) For Marine Corps PA/FOIA issues, DIRPA will coordinate, as appropriate with the Staff Judge Advocate (SJA) to CMC (JAR) and/or Headquarters, Admin Resources Branch (ARAD). The Assistant Chief of Staff Control, Communications, Computer and Intelligence (ACS C4I) is responsible for issues related to security of operations and classified information.

(5) Conduct annual assessments of U.S. Navy or U.S. Marine Corps Web sites to ensure the appropriateness of publicly accessible material and compliance with this instruction.

(6) Establish a mechanism for receiving and reviewing all requests for waivers to provisions of this policy. Waivers will be considered based on provisions of reference (a).

c. CNO, Director of Space, Information Warfare, Command and Control (N6) and United States Marine Corps, Assistant Chief of Staff for Command, Control, Communications, Computers, and Intelligence (ACS C4I) are responsible for establishing procedures to ensure operational integrity and security of the computers and networks supporting DON Web sites. Additionally, CNO (N6) and ACS C4I each will:

(1) Conduct assessments of U.S. Navy or U.S. Marine Corps Web sites at least annually as required by Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (C3I) to ensure compliance with information assurance and security policy requirements.

(2) Notify the affected Major Claimant to ensure the site is either removed from the World Wide Web or brought into compliance when a Web site is not compliant with information assurance and/or security policy requirements.

(3) Maintain overall cognizance for U.S. Navy or U.S. Marine Corps Web sites content-related questions as they pertain to the security of operations or classified information.

(4) Establish a mechanism for receiving and reviewing all requests for U.S. Navy or U.S. Marine Corps waivers to provisions of this policy relating to security of operations or classified information. Waivers will be considered based on provisions of reference (a).

d. DON commands and activities which maintain publicly accessible Web sites will implement and administer a comprehensive Web site program under this instruction. Each addressee who maintains a publicly accessible World Wide Web site as defined in this instruction and reference (a) shall:

(1) Ensure all information currently residing on the command/activity Web site is reviewed by the command/activity public affairs representative and is appropriate for viewing by a worldwide audience, friend and foe alike. Information not suitable for a publicly accessible Web site must either be removed or placed on a restricted-access site.

(2) Develop local procedures for the approval of information posted on command/activity publicly accessible Web sites. At a minimum, this process shall include review by the command's public affairs officer in conjunction with command information assurance personnel, or those at the next appropriate level in the chain of command, to ensure posted information meets requirements set forth in references (a) through (h) and this instruction.

(3) Submit waiver requests via the chain of command to CHINFO/DIRPA or CNO (N6)/ACS C4I, as appropriate.

(4) Designate in writing a primary Web site manager, known as the webmaster. Information on how to contact the webmaster will be included in the command's "home page" source code. At a minimum, the webmaster shall:

(a) Serve as principal point of contact on all technical mafters pertaining to administration of the publicly accessible Web site.

(b) Oversee the commands Web site and ensure compliance with current directives. Oversight includes monitoring the site as often as possible to ensure no unauthorized changes have occurred.

(c) Register the site with the Government Information Locator Service (GILS). GILS identifies public information resources throughout the U.S. Federal government. Registration is accomplished through the appropriate GILS Web site. Under "organizational information," the "Major Component" field will be "United States Navy" or "United States Marine Corps" as appropriate.

(d) Provide training for activity/command personnel on the provisions of reference (a) and this instruction.

RICHARD DANZIG

Distribution:
SNDL, Parts 1 and 2
MARCORPS Codes 71000000000 and 71000000100

## DON WEB SITE ADMINISTRATION

## DEFINITIONS

1. World Wide Web - A part of the Internet displaying text and pictures through the use of computer software called a browser. The World Wide Web originated at the European Laboratory for Particle Physics (CERN) in Geneva, Switzerland.

2. Internet - A network of networks - a world-wide public network that links many smaller networks. No one owns the Internet. It is funded and managed locally within different countries. Having access to the Internet means being able to send and receive e-mail, partake in interactive conferences, access information resources and network news, and transfer files.

3. Web Site - A Web site can be thought of as being similar to a “Welcome Aboard” brochure. It describes the organization and its services, and may be a single page or a collection of related, and linked, pages. Information represented on Department of the Navy pages is considered to be official.

4. Webmaster - The person who maintains a Web page, Web site, and/or the server upon which the Web site resides.

5. Domain - A part of the Domain Name System. The domain to the farthest right is called the top-level domain. The top level domain in “www.navy.mil” is “.mil” which stands for military. The domain name for the U.S. Navy is “navy.mil” and the domain name for the U.S. Marine Corps is “usmc.mil”. Other top-level domains include “.edu”, “.gov”, and “.com”.

6. .HTM, .HTML - The extension for Web documents written in Hypertext Markup Language (HTML) which is the format (code) in which Web pages are written. The extension “signals” the browser (reading software) what type of file to decode and display.

7. Web Page - An HTML document which is usually served by a Web server. Although a Web page usually contains links to other pages, only the information currently being accessed (i.e., viewed) by a Web browser is a part of the current logical page. The logical page is the building block of a WWW document and is composed of text and possibly graphics and multimedia. The term logical is used because unlike a physical piece of paper, a Web page can be as long as needed (from less than one physical page to many physical pages in length). When scrolling down a Web page with a browser, the end of the current page is reached when the scroll bar reaches the bottom.

8. Home Page - The usual or primary starting (entry) point of a World Wide Web (WWW) site.

It is similar to the title page and table of contents of a hard copy document. A home page usually contains links to subsequent (logical) pages in the site. While the home page is the most common access point to a site, it is not the only access point. Any WWW document can be accessed directly from a link or by using its URL (Uniform Resource Locator) address.

9. Source Code - The HTML coding which tags and formats the information to make it viewable by the browser. The source code is not normally viewed by the browser.

10. URL - Uniform Resource Locator. An Internet “address” of a resource. URLs can refer to Web pages, file transfer protocol (FTP) sites or files, Gopher resources, or NNTP (Usenet) Newsgroups. The URLs for pages on the World Wide Web normally begin “http://”.

11. HTTP - HyperText Transfer Protocol is the method by which WWW HTML pages are transferred (served) from the Internet to the local computer’s Web browser and then displayed.

12. Link - A connection from one Web document or file to another, not necessarily within the same Web site. The link typically appears as a word, or phrase, with blue, underlined letters (hypertext). As the cursor touches the link, the cursor takes the form of a hand. Clicking the mouse button causes the Web browser to connect to the document pointed to by the link.

13. Web Browser - Software that acts as a client, allowing a person to retrieve information from various sources, particularly Web servers.

14. Web Server - A software/hardware combination, connected to the Internet, which serves as the “container” for Web sites and is accessed by Web browser software.

## DON WEB SITE ADMINISTRATION

## PUBLICLY ACCESSIBLE WEB SITE POLICY AND PROCEDURES

1. Authority. The establishment of a command Web site on the publicly accessible World Wide Web remains a command prerogative, consistent with other leadership responsibilities for public communication.

a. All DON Web sites must have a clearly articulated purpose, approved by the commander, which supports the command's/activity's mission.

b. Web sites published by Navy/Marine Corps commands but hosted on commercial servers (servers other than "usmc.mil" and "navy.mil") are considered official sites and remain subject to this instruction and reference (a).

c. Publicly accessible Web sites are limited to the command level, i.e. – to that organization with one or more Unit Identification Codes. No separate Web sites will be established for any entity below the command (or command equivalent) level. As example, but not all inclusive, there shall be no departmental or divisional Web sites external to the command's Web site. These departmental/divisional/office pages will reside within the command's Web site.

2. Administration

a. All DON Web sites must be protected from modification on systems exposed to public networks in accordance with references (f) and (g).

b. All command/activity home pages must contain, at a minimum, the following:

(1) Full organizational name.

(2) A statement that the site is an official U.S. Navy or U.S. Marine Corps Web site.

(3) A prominently displayed hypertext link to a tailored Privacy and Security Notice. A statement encouraging visitors to review the security notice is preferred. Overt warning signs or other graphics such as the "skull and crossbones" or "cloak and dagger," or wording indicating danger or warning are specifically forbidden. The tailored Security Notice should be based on the following:

*Notice: This is a U.S. Government Web Site*

*This is a World Wide Web site for official information about [the name of command/activity]. It is provided as a public service by [command/activity name and servicing command if applicable]. The purpose is to provide information and news about the [name of command/activity] to the general public. All information on this site is public domain and may be distributed or copied unless otherwise specified. Use of appropriate byline/photo/image credits is requested.*

*Unauthorized attempts to upload information or change information on this Web site are strictly prohi bited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.*

*For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.*

*Except for authorized law enforcement investigation and to maintain required correspondence files, no other attempts are made to identify individual users or their usage habits. Raw data logs are used to simply determine how many users are accessing the site, which pages are the most popular, and, from time to time, from which top level domain users are coming. This data is scheduled for regular destruction in accordance with National Archives and Records Administration guidelines.*

c. Command Web sites shall contain links to the following sites:

(1) The Navy’s official Web site at http://www.navy.mil and/or the Marine Corps’ official Web site at http://www.usmc.mil.

(2) The parent command, or Immediate Superior In Command (ISIC), home page where applicable.

(3) The Navy and/or Marine Corps recruiting sites at http://www.navyjobs.com and http://www.marines.com.

3. Content

a. All information and photos posted on publicly accessible DON Web Sites must be carefully reviewed to ensure they meet the standards and requirements as published herein.

b. Photos may not be altered in any way. Standard photographic practices of cropping, sizing, dodging, or burning are not considered alteration. Reference (h) applies.

c. In addition to requirements of reference (a), all DON Web Sites shall:

(1) be presented in a manner reflecting the professionalism of the DON;

(2) comply with the Privacy and Freedom of Information Acts, references (d) and (e).

(3) contain only “approved for release” general information suitable for viewing by anyone any place in the world, friend and foe alike.

(4) contain only those images which support the overall mission of the Web site. Images with captioning will only have caption information suitable for viewing by worldwide audience, both internal and external. Captions will comply with DoD/DON policy that names and duty addresses of personnel assigned to units that are sensitive, routinely deployable, or stationed in foreign territories will not be released.

(5) be current, accurate and factual, and reflect only information for which the publishing command has release authority.

d. Specific Web site restrictions include:

(1) Web sites must not include classified material, “For Official Use Only” information, proprietary information, or information that could enable the recipient to infer this type of information. This includes lessons learned or maps with specific locations of sensitive units, ship battle orders, threat condition profiles, etc.). When it is necessary to gain release authority from a senior in the chain of command, subordinate commands will submit material for clearance only after it has been reviewed and necessary amendments made to the fullest capability of the command.

(2) Web sites will not identify family members of DON personnel in any way, nor will family member information be included in any biographies or photos posted to the Web.

(3) Web sites must not include information for specialized, internal audiences. Family Grams, internal news service products and other information may be posted if it is general and suitable for an external audience.

(4) Web sites must not contain any written information or display any logo indicating the Web site is best viewed with any specific Web browser(s); or, that the Web site has been selected as a recommended or featured site by any organization, or, point to any particular search engines or recommend any commercial software. Web sites developed and/or maintained by contractors may not include the contractor's name nor may they link to the contractor's Web site.

(5) Web sites must not contain any material that is copyrighted or under trademark without the specific, written permission of the copyright or trademark holder. Further, the material must relate directly to the command's primary mission. Works prepared by DON personnel as part of their official duties and posted to the command Web site may not be copyrighted, nor may the Web site itself be copyrighted.

(6) Web sites must comply with Department of Defense Freedom of Information Act and Privacy Act requirements regarding the release of names and duty station addresses (both postal and e-mail). Specifically, the names and duty station addresses of individuals who are routinely deployable, overseas, or in a sensitive unit may not be disclosed, except as delineated below. Paragraph 1 4f of reference (e) refers.

(a) Web sites for units that are sensitive, routinely deployable, or stationed in foreign territories shall not display personnel lists, "roster boards," organizational charts, or command staff directories which show individuals' names, individuals' phone numbers or e-mail addresses which contain the individual's name. The exceptions to this policy are flag officers and public affairs officials.

(b) For continental United States-based, non-deployable Echelon 1 and 2 commands, command directories including names and e-mail addresses may be posted on publicly accessible Web sites if deemed by the commander as necessary for the conduct of the command's mission.

(c) For those commands not included in paragraph (b) above, general telephone numbers for commonly requested resources, services, and contacts, without names, are acceptable.

(7) Web sites will not link to non-government sites except as permitted by reference (a). The following external links are specifically authorized:

(a) The U.S. Navy and U.S. Marine Corps official Web sites (http://www.navy.mil and http://www.usmc.mil) may link to Federally chartered, military-related organizations. Commands desiring to link to such Web sites may do so by linking to the U.S. Navy or U.S. Marine Corps official Web sites.

(b) As part of the command's family support function, Web sites of bases, air stations, or equivalent commands may link to local Chambers of Commerce (or overseas equivalents) and local government agencies. Tenant commands should link to the base Web site to provide access to these external links.

(c) Echelon 2 acquisition commands may link to Web sites of partners in industry if that Web site pertains solely to a command program. Links may not be made to the partner's corporate Web site.

(8) No materials or services may be advertised for sale or sold via a command Web site. This includes command memorabilia, ball caps, etc.

(9) Information from other military Web sites will not be duplicated but may be referenced or otherwise linked.

4. Exceptions

a. Educational mission. In instances where the mission of the command includes an educational mission, and where unclassified dissertations or professional papers may be published to the Web for the purpose of peer review, the following disclaimer for exchange of professional information and ideas among scientists, physicians, or educators, must be displayed:

> *"Material contained herein is made available for the purpose of peer review and discussion and does not necessarily reflect the views of the Department of the Navy or the Department of Defense."*

b. Recruiting mission. Navy and Marine Corps Recruiting Web sites reside on ".com" domains. These sites may establish procedures for posting and collecting information which differ from all other DON commands/activities, to include advertising their sites on commercial employment opportunity sites. Exceptions to reference (a) must be coordinated through the chain of command as delineated here and in accordance with reference (a).

5. Interactivity. DON commands/activities may maintain interactive Web sites to the extent that they allow visitors the ability to query the command via electronic mail (e-mail). Commands/activities are cautioned that establishing and maintaining this interactivity can be extremely labor-intensive.

a. Public queries for information should be linked/directed to the site webmaster or public affairs office. Queries should be handled consistent with other written requests for information. Responses shall discuss only those issues within the command's cognizance and shall not violate the release of information provisions of references (d) through (g).

b. Commands may link to the U.S. Navy's "Frequently Asked Questions" page on the official U.S. Navy Web site at http://www.navy.mil. Questions concerning the U.S. Navy or the U.S. Marine Corps as a whole shall also be directed to http://www.navy.mil or http://www.usmc.mil as appropriate.

c. Commands should consider the technical capabilities and needs of their respective audiences when developing the command's Web site. The Information Technology Standards Guide (ITSG) available at http://www.doncio.navy.mil provides guidance for developing a user-friendly Web site.

d. Command Web sites shall not collect personal data (name, address, phone number, etc.) about a visitor without the visitor's expressed permission, nor shall any surveys be conducted on a DON Web site. Any Web site collecting personal information must comply with the provisions of reference (d). Network identification and Internet protocol addresses are not considered personal data.

**DEPARTMENT OF THE NAVY**
**COMMANDER**
**SECOND NAVAL CONSTRUCTION BRIGADE**
**NAVAL AMPHIBIOUS BASE, LITTLE CREEK**
**NORFOLK, VIRGINIA 23521-5070**
**AND**
**COMMANDER**
**THIRD NAVAL CONSTRUCTION BRIGADE**
**PEARL HARBOR, HAWAII 96860-7305**

COMSECONDNCB/COMTHIRDNCBINST 2000.1
N6
**18 NOV 1998**

COMSECONDNCB/COMTHIRDNCB INSTRUCTION 2000.1

Subj: INTERNET POLICY

Ref: (a) DOD Directive 5500.7-R, Section 2-301
(Joint Ethics Regulations)
(b) ALPACFLT/ALLANTFLT 210151Z Feb 98
(c) SECNAV (SECNAV 211930Z Oct 98) Department of the Navy Worldwide Web Policy
(d) OPNAVINST 5239.1A ADP Security Policy
(e) The Privacy Act of 1974, 5 U.S.C. Section 552A

Encl: (1) Sample NAVPERS 1070/613, Administrative Remarks

1. Purpose. To establish COMSECONDNCB/COMTHIRDNCB policy on Internet access and use of Government Information Systems.

2. Background. Information systems and Internet applications can improve many facets of our operations and provide an efficient and effective means of communication and information distribution.

3. Policy

a. COMSECONDNCB/COMTHIRDNCB will promote the widest permissible use of Government Information Systems to access and exchange information in an automated environment. Personnel assigned to NCF units, military and civilian, are encouraged to use their government computers to access the Internet and develop information skills.

b. The best way to develop information technology skills is to get on the Internet and make it the preferred choice to access, develop and exchange information, as supported by reference (a). Fleet policy, as presented in reference (b), is that any permissible use of the Internet enhances the users' professional skills and thus serves a legitimate public interest.

c. Use of Government Information Systems is both an essential work requirement and a personal privilege. All COMSECONDNCB/COMTHIRDNCB personnel are reminded that Commanding Officers and Officers in Charge (CO/OIC) have the authority to control or limit the use of Government Information Systems to include blocking specific sites, limiting or restricting Internet or Email access due to resource constraints, or revoking an individual's use altogether.

d. Permissible use of Government Information Systems is defined as that not prohibited by law, regulation, instruction or command policy. Prohibited uses as derived from reference (a) and amplified in reference (b), include:

(1) Introducing classified information into an unclassified system or environment.

(2) Accessing, storing, processing, displaying, distributing, transmitting or viewing material that is pornographic, racist, promotive of hate crimes, or subversive in nature.

(3) Storing, accessing, processing or distributing classified, propriety, sensitive, For Official Use Only (FOUO) or Privacy Act protected information in violation of established security and information release policies.

(4) Obtaining, installing, copying, pasting, transferring or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret or license agreement.

(5) Knowingly writing, coding, compiling, storing, transmitting or transferring malicious software code, to include viruses, logic bombs, worms and macro viruses.

(6) Promoting partisan political activity.

(7) Disseminating religious materials outside an established command religious program.

(8) Using the system for personal financial gain, such as advertising or solicitation of services or sale of personal property, with the exception of utilizing a command approved

mechanism such as a welfare and recreation electronic bulletin board for advertising personal items for sale.

(9) Promoting or advertising fund raising activities, either for profit or non-profit, unless the activity is specifically approved by the command (e.g. welfare and recreation car washes).

(10) Writing, forwarding or participating in chain letters.

(11) Posting personal home pages.

(12) Personal encryption of electronic communications.

e. Units are encouraged to generate home pages to post unit specific information. Reference (c) outlines the requirements and limitations of Navy home pages. The following specific COMSECONDNCB/COMTHIRDNCB requirements and limitations apply to unit home pages:

(1) <u>Home Page Server</u>. Unit home pages must reside on a military server that is maintained in strict compliance with reference (d) ADP Security Policy.

(2) <u>Brigade Oversight</u>. Unit home pages will be coordinated by Brigade Information Technology Staffs (N6). The Brigade N6's must approve any web site related costs in writing. Units may not directly fund, or accept free, commercial home page services. Units will not provide photographs, articles, logos, history, instructions, or any informational material to any individual or company for the purpose of creating, maintaining, or fostering an unofficial or unauthorized web site. Any unit-originated material published on the Internet must strictly comply with DON worldwide web policy (see reference (c)).

(3) <u>Unit Webmaster</u>. Every unit web site must have a Webmaster and an alternate Webmaster designated in writing by the CO or OIC. The Webmaster is usually either the unit ADP Officer (S6), or the PAO. Online feedback from the web site must be checked daily by the unit Webmaster, or the alternate in the absence of the primary. This is most efficiently done via a direct Email link to the Webmaster.

(4) <u>Posting Information</u>. The unit PAO will screen, edit as necessary, and recommend to the CO/OIC approval/disapproval

for any information (including photos, articles, schedules, cartoons, data etc.) destined to be posted to the home page. The unit CO/OIC must approve all release of information to the home page. The unit Webmaster is the only one authorized to post information to the unit home page, and must develop internal procedures and LAN safeguards to ensure PAO, ADPSO, and CO/OIC approval prior to release of information. COs and OICs are reminded that any information posted to the Internet is a direct reflection on their Command, the Seabees and the Navy. The utmost care must be exercised to ensure all internet "broadcasted" information is appropriate for release and does not compromise unit or force security or personal privacy act protected information (see reference (e) for Privacy Act guidelines).

(5) Periodic Update. Unit COs and OICs are responsible for the quality, timeliness, and relevancy of information posted on their Web site. At least once each month, the Webmaster and PAO will review the entire home page and recommend changes to the CO/OIC. In general, information greater that six (6) months old should be moved to an archive site (6-24 month old info) or incorporated into the unit history section of the home page. The date of the last home page revision will be included with the Webmaster code, name, phone number and Email address.

f. All government computer systems are subject to monitoring, recording, and periodic audits to ensure they are functioning properly and to protect against unauthorized use. Failure to comply with the policy set forth in this instruction or any attempt to disable, defeat, or circumvent security measures may result in disciplinary action.

g. A number of free Email services are available and can be found by conducting an Internet search for free Email. Use of these free services is encouraged for electronically communicating with family and friends when deployed.

h. Although wide use of Internet services are encouraged as described above, there are applications that are detrimental to the operation and efficiency of the unit network. In general, continuous Internet monitoring of hometown radio stations, live sporting events, online news broadcasts, or live video are discourage and should be minimized. These type of applications require a significant bandwidth to operate, slowing the performance of the server, and hindering official business.

4. Action. COs and OICs shall ensure all personnel are familiar with the policies laid out in this instruction. COs and OICs will ensure all personnel review this instruction and receive initial and periodic security awareness and Internet usage training. Such training will be augmented with new and changing issues regarding security and the Internet. An awareness statement and record of training will be signed by all personnel and will be maintained at the command. This training will be documented using appropriate Page 13 entries such as enclosure (1).

S. E. BARKER
Vice Commander

JA Mehula

J. A. MEHULA
Deputy Commander

Distribution:
COMSECONDNCB/COMTHIRDNCBINST 5216.1B
Lists I & II

ADMINISTRATIVE REMARKS
NAVPERS 1070/613(Rev.10-81)
S/N 0106-LF-010-6991

Command Name, Address, UIC

**DDMMMYY**: I have read the command's Internet instruction and received Internet security and usage training. I fully understand the terms of this policy and agree to abide by them. I realize that command resources are subject to monitoring and that the Internet address of any site that I visit is recorded. I am aware that any use which is illegal, harassing, offensive and/or in violation of other command policies may be the basis for criminal, disciplinary, and administrative action.

Member signature: ______________________________

Instructor signature: ______________________________

| | | |
|---|---|---|
| NAME (Last, First, MI) | SSN | BRANCH & CLASS |

Canc frp:

COMSECONDNCB/COMTHIRDNCBNOTE 2000
N6

COMSECONDNCB / COMTHIRDNCB NOTICE 2000

Subj: WEB SITE ADMINISTRATION

Ref: (a) COMSECONDNCB/COMTHIRDNCBINST 2000.1, "Internet Policy,"
(b) DOD Policy Memorandum, "Web Site Administration," 07 Dec 98
(c) SECNAVINST 5720.47, "DON Policy for Content of Publicly Accessible World Wide Web Sites"
(d) "NCF Webmaster Resource Center" < http://www.seabee.navy.mil/help/>

Encl: (1) Webmaster Designation Letter

1. **Purpose**. To provide guidance and assign responsibility for administering and maintaining an unclassified, publicly accessible Web information service.

2. **General**. References (a) through (c) are governing policies for managing and administering publicly accessible Web sites. Reference (d) provides a central resource to all NCF Webmasters. This notice provides additional guidance in reference to Command responsibilities and information deemed inappropriate for publication on the NCF publicly accessible Web Domain.

3. **Responsibility**.

a. It is the responsibility of the CO/OIC to ensure designated Webmasters and PAO staffs are familiar with the content of this notice as well as references (a) through (c).

(1) **Command Responsibilities**

(a) Create Letters of Designation for all primary and alternate Webmasters. (Enclosure 1)
(b) Approve and publish information that only your Unit generates (approval restricted to the Unit CO/XO/OIC).
(c) Ensure all information placed on publicly accessible Web sites is properly reviewed for security, levels of sensitivity and other concerns before it is published to the web site.
(d) Ensure reasonable efforts are made to verify the accuracy, consistency, appropriateness, and timeliness of all information placed on the Web site.

(e) Establish procedures for management oversight and regular functional review of the Unit Web site.
(f) Use only non-copyrighted material, text, clip art, hypertext links, images and sound or video clips and only if they directly relate to the Unit's mission.
(g) Ensure all outdated or superseded information is identified and promptly removed from the active Web site or appropriately archived.
(h) Ensure availability of a suitable workstation with LAN/ Internet access for Web site administration.
(i) Do not maintain or provide information or pictures to an unofficial Web site.

(2) **<u>Webmaster Responsibilities</u>**

(a) Review reference (d). (Web site contains relevant instructions, FAQ, Computer Based Training and more)
(b) Provide "ALT" tags (description in the “Image Properties”) for all images posted on web pages.
(c) Place all text and graphics inside a table not to exceed 450 pixels wide.
(d) Provide a caption associated with all photos.
(e) Ensure page content uses #2 (10 pt) Verdana, Arial font.
(f) Ensure GILS registration information is kept current. <http://www.defenselink.mil/locator/>
(g) Ensure the "Custom" information in “File”, "Page Properties" is kept current with the changing of personnel.
(h) Spell check all pages with FrontPage Explorer to ensure all web pages maintain a professional appeal.

4. **<u>NCF Web Page Restrictions</u>**

a. In keeping with a "One NCF" concept, alterations to the following areas are unauthorized.

(1) Links on the left side menu may not be removed or renamed, although two user-defined links may be added between the "augment " and "archive" links. (**Exception**: Active links may be unlinked if not in use)
(2) Alterations to imagemap hotspots in the Unit’s banner are not permitted.
(3) Use of "frames technology" on the NCF domain is unauthorized.
(4) Alterations to the Unit Home Page are not permitted, except to update the CO/XO/CMC/OIC/AOIC.
(5) While DOD links are encouraged, care must be taken to ensure they are properly linked prior to publishing on the Domain. Providing a page for external links is discouraged because one has been established and is maintained by the NCF Webmaster.
(6) Although the use of scrolling marquees, Active X controls and JAVA applets is not forbidden, they are discouraged because of their limitations with older browsers.

5. **DOD Web Page Restrictions**

a. In accordance with reference (c) the following types of information is restricted from a publicly accessible web site.

(1) News and Family Grams designated for a specific or internal audience can be published on the Web provided names associated with pictures, phone numbers and pictures of family members are removed.

(2) Non-government/ DOD links is not permitted regardless of whether or not a disclaimer is provided. This includes Command Alumni Web sites, etc. Command Augment Units are not permitted to have unofficial Home pages. The "Augment" link is provided for this purpose.

(3) With exception to the CO, XO, C/MC, Command OIC, AOIC and PAO's, photos with names are not permitted on DOD Web pages. Personnel are only referenced via their rate or as Seabee. This applies to any routinely deployable Unit, which includes all NCF Units. (An additional exception is a Flag Officer who may be referenced by rank and name.)

(4) Direct points of contact (phone, e-mail or mailing address) are not permitted, unless it is designated as a central point of contact, but may not be associated with a specific person's name. This includes the Command suite and FSC.

(5) Pictures, names or any reference to family members are not permitted at any time. This includes the OMBUDSMAN. The position may be referenced by title only.

(6) Detailed maps or installation photography are not permitted. (Especially when deployed in a foreign country.)

(7) Maps or directions to bases from airports, bus stations etc, are the responsibility of the Home Station and not the Tenant Command. Links shall be directed to their web pages for this type of information.

(8) Only Home Station Web sites can provide links to the local Chambers of Commerce (or overseas equivalents) and local government agencies.

6. **Restricted Content**

a. Guidance is provided to identify information that may be inappropriate for posting to publicly accessible web sites. (These restrictions include, but are not limited to, the following.)

(1) Military Operations & Exercises information

(a) Unit Organization
(b) Unit readiness specifics
(c) Detailed mission statement
(d) Specific Unit phone/fax numbers (secure and unsecured)
(e) Time-Phase Force Deployment Data (TPFDD)
(f) Ops schedules
(g) Logistics support requirements
(h) Transportation
(i) Munitions
(j) Force Apportionment
(k) Force Allocation
(l) Unit Bed-down information
(m) Unit Recall Rosters

(2) Personal Information

(a) Names associated with pictures other than CO/XO/C/MC/SOY/SOQ
(b) Social security numbers
(c) Dates, cities and states of birth
(d) Home addresses
(e) Telephone numbers other than duty office numbers
(f) Information which would be a clearly unwarranted invasion of personal privacy

(3) Other

(a) FOR OFFICIAL USE ONLY (FOUO) information
(b) Advertising or product promotion
(c) Links to non-official or password protected web sites
(d) Use of copyrighted material is not permitted without express written permission from the originating author

[Joint Signature}

1300
Ser [*/*]
[Date]

From: Commanding Officer/ Officer in Charge, [Unit]
To: [Designating Individual]

Subj: DESIGNATION AS [COMMAND] WEBMASTER

Ref: (a) SECONDNCB/THIRDNCBINST 2000.1, Internet Policy, 18 Nov, 98.
(b) SECNAVINST 5720.47, Department of the Navy Policy for the Content of Publicly Accessible World Wide Web Sites, 01 July, 99**.**
(c) DOD Policy Memorandum, "Web Site Administration" Dec 7, 98.
(d) http://www.seabee.navy.mil/help, NCF Webmaster Resource Center.

1. Per reference (a), You are hereby designated as the [Command] Webmaster.

2. You are further directed to familiar yourself with the contents and administrative policies of reference (a) through (c). Reference (d) is the Webmaster Resource Center. Site contains above listed references, training material, FAQ and general information.

3. Responsibilities:

   a. Serve as principle point of contact for all technical matters pertaining to the publicly accessible Web site.
   b. Oversee the Commands Web site and ensure compliance with current directives.
   c. Monitor the site to ensure no unauthorized changes have occurred.
   d. Coordinate with the NCF Webmaster for changes to current policies or when experiencing difficulties in administering your Web site.

4. This designation terminates with your detachment from this Command, or when relieved, whichever occurs first.

[CO/OIC signature]

Copy to:
Brigade N6's
NCF Webmaster
Service Record

Enclosure (1)

COMSECONDNCB/COMTHIRDNCBINST 5780.1
N6

COMSECONDNCB / COMTHIRDNCB INSTRUCTION 5780.1

Subj: NCF INTRANET / INTERNET POLICY GUIDELINES

Ref: (a) "NAVFAC Intranet Style Guide"
(http://navfacilitator.navfac.navy.mil/about/stylegui.htm)
(b) DOD Policy Memorandum, "Web Site Administration," 07 Dec 98
(c) SECNAVINST 5720.47, "DON Policy for Content of Publicly Accessible World Wide Web Sites," 01 Jul 99
(d) COMSECONDNCB/COMTHIRDNCBINST 2000.1, "Internet Policy," 18 Nov 98
(e) Assistant Secretary of Defense Memorandum, "Policy Guidance for use of Mobile Code Technologies in DOD Information Systems," 07 Nov 00
(f) "NCF Webmaster Resource Center" (http://www.seabee.navy.mil/help/)

Encl: (1) Naval Construction Force Internet Policies/Procedures
(2) Naval Construction Force Intranet Policies/Procedures
(3) Sample Webmaster Designation Letter
(4) Command Internet Website Template (http://www.seabee.navy.mil/web_template)
(5) Command Intranet Website Template (http://ncf.navfac.navy.mil/unit_template)
(6) Forward Deployed Camp Template (http://ncf.navfac.navy.mil/camp_template)

1. **Purpose**. To implement references (a) through (e) within the Naval Construction Force and provide additional policies.

2. **Cancellation**: COMSECOND/COMTHIRDNCB NOTICE 2000, Website Administration.

3. **Scope**: This instruction is applicable to Websites designed, developed, procured, or managed on the NCF Domain.

4. **Background**: The appearance, accuracy, and relevance of information presented by these websites reflect the NCF's professional standards and credibility. References (b) and (c) identify content restrictions on publicly accessible websites and makes recommendations based on information prior to the release of reference (d). This instruction will identify requirements specified in references (a) through (e).

5. **Policy**: Reference (a) provides the primary guidance governing standards as set by NAVFAC for publishing or posting information to the NAVFAC Intranet. Reference (b) is the primary governing policy for all unclassified World Wide Websites. Reference (c) provides guidance to the Navy regarding information appropriate for dissemination to the publicly accessible World Wide Web. Reference (d) is the joint Second / Third NCB Internet Policy. Reference (e) is the DOD Mobile Code Policy concerning the use and potential

restrictions of ActiveX®, Java™ applets, and JavaScript. Reference (f) is the Webmaster Resource Center located on the Seabee Internet Help web. Website provides tutorials, troubleshooting assistance as well as the PKI certificates. Enclosure 1 identifies NCF policy and procedure with regards to the publicly accessible Internet web sites. Enclosure 2 identifies policy and procedures with regards to the NCF Intranet web sites. Enclosure 3 is a Webmaster Designation letter template mandated by references (b), (c), and (d). Enclosure 4 is the NCF approved publicly accessible web sites template. Enclosure 5 is the NCF approved Unit Intranet web sites template. Enclosure 6 is the NCF approved forward deployed camp Intranet web sites template.

6. **Definitions**: Terms used in this instruction are defined in reference (c).

7. **Action**:

a. Construction Battalion Center Port Hueneme N6 is the governing authority over all matters concerning the design, implementation, specification, and application rollout with regards to both the NCF Internet and Intranet domains. They will also provide final interpretation of this instruction in the event of a dispute.

b. All NCF Commands and constituents hosting a website on either the NCF Internet or Intranet will ensure compliance with this instruction as well as references (a) through (e).

c. The NCF Enterprise Webmaster will periodically review all websites and notify the appropriate Command if noncompliant of NCF established policy. The NCF Webmaster shall deactivate any and all websites that continue to be noncompliant after 10 calendar days following notification. The C4I QMB shall be briefed quarterly as to the state of the webs, domain statistics, and related issues.

d. Change requests shall be addressed to the CBCPH N6 for approval.

e. Application development shall conform to NAVFAC standards. ColdFusion is the only application software supported on the NCF Web Servers. ASP is disabled as directed by NAVFAC.

8. **NCF Software Standards**:

a. Microsoft Office 97 suite
b. Adobe Acrobat 4
c. FrontPage 2000
d. ColdFusion 4.01

W. M. McKerrall
Chief of Staff

J. D. Rice
Chief of Staff

Distribution:
COMTHIRDNCB / COMSECONDNCBINST 5216.1C
(List I – IV)

## NAVAL CONSTRUCTION FORCE INTERNET POLICY GUIDELINES

1. **General**. The publicly accessible NCF Internet sites (http://www.seabee.navy.mil/) provide general information about the Seabees, their mission, and their role in the United States Navy / Marine Corps.

2. **Policies**: Visitors to the NCF websites should experience the "One NCF" concept.

   a. All publicly accessible websites hosted on the NCF Domain (http://www.seabee.navy.mil/) shall adhere to references (b) through (e).

   (1) Modifications to the following are not permitted without the express authorization of the NCF C4I QMB.

   (a) Approved NCF template (top banner, left menu and footer)
   (b) NCF Unit home page.
   (c) The "Links" hyperlink on the "Left Menu" or "Site Map".

   (2) A designation letter (enclosure 3) shall be prepared for both the primary and alternate Webmasters as directed by references (b) through (d).

   (3) Local procedures shall be prepared indicating the approval process of all information posted to a publicly accessible website.

   (4) Information shall not be archived longer than 6 months.

3. **Responsibilities**:

   a. Command Responsibilities

   (1) Approve and publish information for which your Unit is responsible (approval restricted to the Unit CO/XO/OIC).
   (2) Ensure all information placed on publicly accessible websites is properly reviewed for security, levels of sensitivity, and other concerns.
   (3) Ensure reasonable efforts are made to verify the accuracy, consistency, appropriateness, and timeliness of all information.
   (4) Establish procedures for management oversight and regular functional review of the Unit website.
   (5) Use non-copyrighted material (e.g. text, clip art, images, etc) unless express written consent is obtained from the creator/owner.
   (6) Limit content to material (e.g. text, clip art, images, etc) that directly support the Unit mission.
   (7) Ensure all outdated or superseded information is identified and promptly removed or appropriately archived.

(8) Ensure availability of a suitable workstation with LAN / Internet access for website administration.
(9) Do not host or provide Unit information to any unofficial websites.

b. Webmaster Responsibilities

(1) Regularly review reference (f). (Website contains relevant instructions, FAQ, Computer Based Training, and more.)
(2) Provide "ALT" tags (Image Properties / Alternative Representation) for all images posted on web pages.
(3) Place all text and graphics inside a table not to exceed 450-pixels in width.
(4) Provide a caption associated with all photos.
(5) Ensure all text is formatted to use the fonts of Verdana, Arial, #2, (10 pt).
(6) Ensure Government Information Locator Service (GILS) registration information is kept current. (http://sites.defenselink.mil/)
(7) Ensure the "Custom" information in "File", "Page Properties", and "Custom" tab is kept current with the changing of personnel.
(8) Spell check all pages with FrontPage prior to publishing to the domain server.

## 4. NCF Website Restrictions

a. In keeping with a "One NCF" concept, alterations to the following areas are not permitted.

(1) Links on the left side menu may not be removed or renamed. However, up to two user-defined links may be added between the "Augment" and "Archive" links. (**Exception**: Active links may be unlinked if not in use.)
(2) Image Map Hotspots located in the Unit banner are not to be altered.
(3) Use of "frames" on any publicly accessible website is unauthorized.
(4) Alterations to the Unit Home Page are not permitted, except to update the CO/XO/CMC/OIC/AOIC.

b. Although providing links to other DOD activities is authorized, it is recommended the NCF Webmaster place any desired links on the "links.htm" page. Providing links to other activities requires regular maintenance to ensure the active links are valid. Activities have a tendency to move or delete pages on their Web servers without prior notification.

c. The use of scrolling marquees, ActiveX, Java applets, and JavaScript are unauthorized on NCF publicly accessible websites. Restriction of these controls is vital due to current Fleet Firewall and the DOD Mobile Code Policies.

## 5. Naming Conventions:

a. Adherence to the specified naming conventions is vital to the safe recovery of data as well as preventing complications for the viewers. Names with spaces, as well as the use of unsafe or reserved characters, cause problems with some Web browsers and data storage protection on the servers.

(1) File and Folder names:

(a) File and folder names are primarily for the use of the website author as a point of reference for information contained within and for no other purpose.

(b) File and folder names aren't required to meet the 8.3 (DOS) standard, but this policy expressly mandates that they do not exceed 25 characters in length.

(2) Illegal use of restricted characters:

(a) There are a number of characters identified as unsafe for use or reserved for other purposes and should not be used in file or folder names. The following characters are restricted from use on the NCF Internet Web Server.

1) Restricted Characters:

Unsafe Characters:

1. Space
2. < >
3. "
4. #
5. %
6. {}
7. ?
8. |
9. \
10. ^
11. ~
12. []

Reserved Characters:

1. ;
2. /
3. ?
4. :
5. @
6. =
7. &

Special Characters:

1. $
2. -
3. .
4. !
5. *
6. '
7. ()
8. ,
9. "

6. **Website Maintenance**:

a. Websites inherently require regular maintenance to ensure content is relevant, hyperlinks are valid, and information is appropriately archived. The primary goal of any Webmaster should be to organize the web initially to reduce the frequency changing data location, risking broken links and inaccessible pages.

(1) The following maintenance shall be performed prior to publishing web pages to the Internet web server.

(a) Data is compliant with Enclosure (1), Section (5).
(b) Hyperlinks are verified and broken links corrected.
(c) Outdated information is removed or appropriately linked.
(d) Entire web is spell checked.
(e) Information is approved for public release.

7. **DOD Web Page Restrictions**

a. In accordance with reference (c) the following types of information are restricted on a publicly accessible website.

(1) All private websites requiring a logon and password (NCF Friends and Family Webs) must require the use of SSL encryption using the DOD PKI certificate for access.

(2) News and Family Grams designated for a specific or internal audience can be published on the Web provided names associated with pictures, phone numbers, and pictures of family members are removed.

(3) Non-government/ DOD links are not permitted regardless of whether or not a disclaimer is provided. This includes Command Alumni Web sites, etc. Command Augment Units are not permitted to have unofficial Home pages. The “Augment” link is provided for this purpose.

(4) With exception to the CO, XO, C/MC, Command OIC, AOIC and PAO’s, photos with names are not permitted on publicly accessible web pages. Personnel are only referenced via their rate or as “Seabee”. This applies to any routinely deployable Unit, which includes all NCF Units. (An additional exception is a Flag Officer who may be referenced by rank and name.)

(5) Direct points of contact (phone, e-mail, or mailing address) are not permitted, unless it is designated as a central point of contact, but may not be associated with a specific person’s name. This includes the Command suite and FSC and RSS Supervisors.

(6) Pictures, names, or any reference to family members are not permitted at any time. This includes the OMBUDSMAN and the staff biographies. The OMBUDSMAN position may be referenced by title only.

(7) Detailed maps or installation photography are not permitted. (Especially when deployed on foreign soil.)

(8) Maps or directions to bases from airports, bus stations, etc are the responsibility of the Home Station and not the Tenant Command. Links shall be directed to their web pages for this type of information. Directions are permitted from the front gate to the Unit compound only.

(9) External links to non-DOD websites are prohibited. Links to local government organizations are the responsibility of the Home Station.

b. Restricted Content

(1) Guidance is provided to identify information that may be inappropriate for posting to publicly accessible websites. (These restrictions include, but are not limited to, the following.)

(a) Military Operations & Exercises Information

1) Unit Organization
2) Unit readiness specifics
3) Detailed mission statement
4) Specific Unit phone/fax numbers (secure and unsecured)
5) Time-Phase Force Deployment Data (TPFDD)
6) Ops schedules
7) Logistics support requirements
8) Transportation
9) Munitions
10) Force Apportionment
11) Force Allocation
12) Unit Bed-down information
13) Unit Recall Rosters

(b) Personal Information

1) Names associated with pictures other than CO/XO/C/MC/SOY/SOQ
2) Social security numbers
3) Dates, cities, and states of birth
4) Home addresses
5) Telephone numbers other than duty office numbers
6) Information which would be a clearly unwarranted invasion of personal privacy

(c) Other

1) FOR OFFICIAL USE ONLY (FOUO) information
2) Advertising or product promotion
3) Links to non-official or password protected web sites. (F&F websites are an exception to this rule)
4) Use of copyrighted material is not permitted without express written permission from the originating author

8. **Online Applications**: Applications are designed to simplify and streamline the business practices of the NCF. All applications are developed with Allaire's ColdFusion 4.01 or above. For information on current or upcoming applications, visit http://ncf.navfac.navy.mil/apps.htm.

a. Administrative:

(1) Administrative accounts can be requested for certain applications providing specific user rights necessary to input Unit information.

(2) Application development can be requested via an online form at http://ncf.navfac.navy.mil/cfw/. Prior to any development, approval must be coordinated via the NCF C4I QMB.

(3) All access accounts must be requested via the NCF Webmaster (ncfwebmaster@nitc.navfac.navy.mil) using the following format:

(a) **Command**:
(b) **Rate/Rank/Civ. grade**:
(c) **Full Name**: (First, MI, Last)
(d) **E-mail Address**:
(e) **Phone**:
(f) **DSN**: (if available)

b. Photo Library:

(1) The photo library is a repository of Seabee action photos that can be displayed on the Seabee Internet (www.seabee.navy.mil). The application provides a means for the Unit PAO or designated person/s to upload photographs to the Seabee Internet Home Pages. The application is accessible at (https://www.seabee.navy.mil/photos/)

(a) All photographs posted to the publicly accessible websites must meet the following minimum requirements:

1) No unsafe acts depicted
2) Appropriate safety gear worn by all personnel depicted in photograph

3) No lewd or disgusting photos
4) No photographs that would detract or discredit the NCF.
5) All photographs shall be at least 600-pixels in width

c. Account Management:

(1) The Account Management application simplifies maintenance of individual user accounts required to post information to the NCF Internet / Intranet. System policies require all accounts be updated a minimum of every 90 days.

(a) Users will be notified via e-mail 15 days prior to account expiration and each day thereafter until the account has been updated.
(b) The primary Webmaster for each Unit will receive notification when the Friends and Family account is within its 15-day expiration window as well.
(c) Application access is available at https://www.seabee.navy.mil/passwd/. Follow the online instructions.

## NAVAL CONSTRUCTION FORCE INTRANET POLICY GUIDELINES

1. **General**. The NCF Intranet is an official business-only website. The primary purpose is to provide information that will help streamline the business practices of the NCF. Its intended purpose is to provide a means of posting information that may be archived and retrieved by authorized users with ease.

2. **Policies**: This instruction as well as reference (a) shall be the governing policies for all aspects of the NCF Intranet. In the event of a dispute, the CBCPH N6 shall be responsible for the final interpretation of this instruction.

   a. Templates:

      (1) All NCF Units as well as constituents are required to maintain their respective websites in accordance with enclosures (5) and (6). Deviation from the approved template design complicates the navigation throughout the NCF Intranet defeating its intended purpose.

   b. Formatting:

      (1) The Intranet is a compilation of current and archived information for past, present, and future reference. To eliminate the problems associated with backwards compatibility, software standards have to be adhered to when publishing information.

         (a) Word / Excel Documents:

            1) Documents shall be converted to PDF format using Adobe Acrobat and hyperlinked from an web page.
            2) Spreadsheets, as well as Excel workbooks, shall be converted to PDF prior to publishing.
            3) Documents requiring an update or change for a specific period of time shall remain in its native format and converted to PDF once archived.

         (b) HTML Pages

            1) Documents created in HTML shall use Verdana, #2 (10pt) font.
            2) Each page shall include the a) NAVFAC header and footer and b) NCF banner.
            3) All data shall reside in a base table not to exceed 585-pixels.

         (c) PowerPoint Presentations

1) PowerPoint presentations shall be converted to a non-frames HTML presentation.
2) The original presentation shall be made available for download at the viewer's convenience.

c. Naming conventions:

(1) Adherence to the specified naming conventions is vital to the safe recovery of data as well as preventing complications for the viewers. Names with spaces, as well as the use of unsafe or reserved characters, cause problems with some Web browsers and data storage protection on the servers.

(a) File and Folder names:

1) File and folder names are primarily for the use of the website author as a point of reference for information contained within and for no other purpose.

2) File and folder names aren't required to meet the 8.3 (DOS) standard, although this policy expressly mandates that they do not exceed 25 characters in length.

(b) Illegal use of restricted characters:

1) There are a number of characters identified as unsafe for use or reserved for other purposes and should not be used in file or folder names. The following characters are restricted from use on the NCF Intranet Web Server.

a) Restricted Characters:

Unsafe Characters**:**

1. Space
2. < >
3. "
4. #
5. %
6. {}
7. ?
8. |
9. \
10. ^
11. ~
12. []

Reserved Characters:

1. ;
2. /
3. ?
4. :
5. @
6. =
7. &

Special Characters:

1. $
2. -
3. .
4. !
5. *
6. '
7. ()
8. ,
9. "

d. Website Maintenance: Websites inherently require regular maintenance to ensure content is relevant, hyperlinks are valid, and information is appropriately archived. The primary goal of any Webmaster should be to organize the webs initially to reduce the frequency of having to change data location, risking broken links and inaccessible pages.

(1) The following maintenance shall be performed prior to publishing web pages to the Intranet web server.

(a) Data is compliant with Enclosure (2), Section (2.c.).
(b) Hyperlinks are verified and broken links corrected.
(c) Outdated information is removed or appropriately linked.
(d) Entire web is spell checked.
(e) Information is approved for release.

6. **Online Applications**: Applications are designed to simplify and streamline the business practices of the NCF. All applications are developed with Allaire's ColdFusion 4.01 or above. For information on current or upcoming applications, visit http://ncf.navfac.navy.mil/apps.htm.

a. Administrative:

(1) Administrative accounts can be requested for certain applications providing specific user rights necessary to input Unit information.

(2) Application development can be requested via an online form at http://ncf.navfac.navy.mil/cfw/. Prior to any development, approval must be coordinated via the NCF C4I QMB.

(3) All access accounts must be requested via the NCF Webmaster (ncfwebmaster@nitc.navfac.navy.mil) using the following format:

(a) **Command**:
(b) **Rate/Rank/Civ. grade**:
(c) **Full Name**: (First, MI, Last)
(d) **E-mail Address**:
(e) **Phone**:
(f) **DSN**: (if available)

b. Document Library:

(2) The document library is a central repository for all NCF Unit instructions, notices, etc. The application can be accessed at http://navfacilitator.navfac.navy.mil/ncf/docs/. All documents must be converted to PDF format prior to uploading.

(a) The following information is required when uploading a document:

1) **Publication Type*:** (Instruction, MOA, MOU, notice, or publication)
2) **Document No.*:** (5780)
3) **Change Version: (.1, .2b, etc)**
4) **Code*:** (Command)
5) **Date*:** (Day/Month/Year)
6) **Document Title*:** (self explanatory)
7) **POC:** (self explanatory)
8) **Keywords:** (self explanatory)
9) **Status*: Active** (no answer required)
10) **Target Audience*: Intranet** (no answer required)
11) **File to Upload:** (Select file from local drive)
12) **File to Upload:** (Select file from local drive)

**Note:** Information depicted with an asterisk is required. [because I'm sure it will be printed on a B&W printer.]

c. Account Management:

(1) The Account Management application simplifies maintenance of individual user accounts required to post information to the NCF Internet / Intranet. System policies require all accounts be updated a minimum of every 90 days.

(a) Users will be notified via e-mail 15 days prior to account expiration and each day thereafter until the account has been updated.
(b) The primary Webmaster for each Unit will receive notification when the Friends and Family account is within its 15-day expiration window as well.
(c) Application access is available at https://www.seabee.navy.mil/passwd/.
(d) Follow the online instructions.

1300
Ser [*/*]
[Date]

From: Commanding Officer/ Officer in Charge, [Unit]
To: [Designating Individual]

Subj: DESIGNATION AS [COMMAND] WEBMASTER

Ref: (a) SECONDNCB/THIRDNCBINST 2000.1, “Internet Policy,” 18 Nov 98
(b) SECNAVINST 5720.47, “DON Policy for Content of Publicly Accessible World Wide Web Sites,” 01 Jul 99
(c) DOD Policy Memorandum, “Web Site Administration,” 7 Dec 98
(d) NCF Webmaster Resource Center, http://www.seabee.navy.mil/help/

1. Per reference (a), you are hereby designated as the [Command] Webmaster.

2. You are further directed to familiarize yourself with the contents and administrative policies of reference (a) through (c). Reference (d) is the NCF Webmaster Resource Center. This site contains above listed references, training material, FAQ, and general information.

3. Responsibilities:
   a. Serve as principle point of contact for all technical matters pertaining to the publicly accessible Website.
   b. Oversee the Command’s Website and ensure compliance with current directives.
   c. Monitor the site to ensure no unauthorized changes have occurred.
   d. Coordinate with the NCF Webmaster for changes to current policies or when experiencing difficulties in administering your Website.

4. This designation terminates with your detachment from this Command, or when relieved, whichever occurs first.

[CO/OIC signature]

Copy to:
Brigade N6’s
NCF Webmaster
Service Record

**ASSISTANT SECRETARY OF DEFENSE**
**6000 DEFENSE PENTAGON**
**WASHINGTON, DC 20301-6000**

November 7, 2000

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF THE DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS AND SERVICES
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS, JOINT STAFF
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES

SUBJECT: Policy Guidance for use of Mobile Code Technologies in Department of Defense (DoD) Information Systems

Mobile code[1] is a powerful software tool that enhances cross-platform capabilities, sharing of resources, and web-based solutions. Its use is widespread and increasing in both commercial and government applications. In DoD, mobile code is employed in systems supporting functional areas ranging from acquisition to intelligence to transportation. Mobile code, unfortunately, has the potential to severely degrade DoD operations if improperly used or controlled.

[1] Mobile code is software obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.

To protect DoD systems from the threat of malicious or improper use of mobile code, we must assess and control the risks imposed by the technology. The guidance in Enclosure 1 is the first step in an iterative process to reduce such risks to DoD information systems. It categorizes mobile code technologies and restricts their application within DoD based on their potential to cause damage if used maliciously. It is applicable to all DoD information systems used to process, transmit, store, or display DoD information, including commercial off-the-shelf (COTS) products and electronic commerce applications used but not owned by the government. Excepted are Special Access Program and Sensitive Compartmented Information systems and networks, laboratory or test-bed networks which cannot communicate directly with other networks, and application software components where the installation, network transferal and execution of the application is conducted totally within a single security enclave.

Testing of the controls imposed by Enclosure 1 to date has revealed minimal negative effects on DoD information systems, functions, and operations. However, additional in-depth operational testing will be conducted before this memorandum transitions to a formal DoD directive to ensure that no unintended consequences preclude conduct of any of the Department's legitimate functions, to include administrative, as well as mission critical and mission support activities. The test results will be distributed as they become available.

During the transition period, all DoD Components are directed to follow the policy guidance at Enclosure 1 as closely as possible. In those instances where the policy cannot be followed because of unacceptable documented consequences to mission, the Component Head (including OSD Principal Staff Assistants) responsible for the system or application in question shall ensure that the DoD CIO is informed of the use of the non-conforming mobile code, along with an assessment of associated risk and any known mitigation measures. The DoD CIO will in turn ensure that this information is provided to all affected DoD Components.

Definitions of terms used in this memorandum and associated material are at Enclosure 2. My point of contact for this policy guidance is Mr. Donald L. Jones in the Office of the Director for Infrastructure and Information Assurance at (703) 614-6640 or e-mail donald.l.jones@osd.pentagon.mil. For technical questions contact Lt Col Danny A. Flowers, Joint Staff Command, Control, Communications, and Computer (C4) Systems Directorate (J-6), Information Assurance Division (J6K) at commercial (703) 693-4578 or DSN 223-4578, e-mail danny.flowers@js.pentagon.mil.

Arthur L. Money

Attachments

## Enclosure 1
## Mobile Code Technology Risk Categories and Use Restrictions

1. The following paragraphs categorize and define mobile code technologies used within DoD based on risk, and restrict their application based on their potential to cause damage if used maliciously. Initial risk category assignments for commonly used mobile code technologies are listed in Attachment 1. Configuration guidance will be provided separately.

1.1. Category 1.

1.1.1. Category 1 mobile code technologies exhibit a broad functionality, allowing unmediated access to workstation, host and remote system services and resources. Category 1 mobile code technologies have known security vulnerabilities with few or no countermeasures once they begin executing. Execution of Category 1 mobile code typically requires an all or none decision, either execute with full access to all system resources or don't execute at all.

1.1.2. Category 1 mobile code technologies can pose a severe threat to DoD operations. However, the implementations of some mobile code technologies differentiate between *signed* and *unsigned* mobile code. These implementations can be configured to allow the execution of *signed* mobile code while simultaneously blocking the execution of *unsigned* mobile code. When Category 1 mobile code is *signed* and obtained from a trusted source, the risk is reduced.

1.1.3. Category 1 mobile code may be used in DoD information systems only when the mobile code is *signed* with a DoD-approved PKI code signing certificate and the mobile code is obtained from a trusted source. Until a DoD-approved PKI code-signing certificate is available, the responsible CIO may approve alternate commercially available code signing certificates.

1.1.4. To the extent possible, all DoD computer systems (e.g., hosts), workstations, and applications capable of executing mobile code shall be configured to disable the execution of *unsigned* Category 1 mobile code obtained from outside the enclave boundary. In situations where the use of *unsigned* Category 1 mobile code is critical to the performance of a mission, a written waiver for its use may be approved by the responsible CIO. The waiver should stipulate use of a mobile code security product, along with a security configuration for the product, to mitigate the risk posed by the *unsigned* category 1 mobile code. Until such time as mobile code security products validated by the National Information Assurance Partnership (NIAP) as specified in National Security Telecommunications and information Systems Security Policy (NSTISSP) Number 11 are available, the responsible CIO may approve the use of specific commercial-off-the-shelf (COTS) third party mobile code security products when granting a waiver for *unsigned* Category 1 mobile code use. The waiver shall be attached to the accreditation package as part of the System Security Authorization Agreement (SSAA) required by DoDI 5200.40.

1.1.5. All program offices with new procurement and development efforts that rely on Category 1 mobile code technologies (*signed* or *unsigned* w/waiver) shall include a mobile code risk mitigation strategy detailing the measures incorporated into the system development to curtail the risk posed by its use as part of their risk management plan, in accordance with DoDI 5200.40. The risk mitigation strategy shall be included in the accreditation package as part of the SSAA. No new DoD program may expend funds on the development or procurement of products or services that contain, use, or depend on the download and execution of Category 1 mobile code across enclave boundaries, unless that product or service uses *signed* mobile code as stipulated in paragraph 1.1.3. above.

1.2. Category 2

1.2.1. Category 2 mobile code technologies have full functionality, allowing mediated or controlled access to workstation, host, and remote system services and resources. Category 2 mobile code technologies may have known security vulnerabilities but also have known fine-grained, periodic, or continuous countermeasures or safeguards.

1.2.2. Category 2 mobile code technologies can pose a moderate threat to DoD information systems. The use of Category 2 mobile code technologies, when combined with prudent countermeasures against malicious use, can afford benefits that outweigh their risks.

1.2.3. Category 2 mobile code may be used in DoD information systems if the mobile code is obtained from a trusted source over an assured channel. In addition, *unsigned* Category 2 mobile code, whether or not obtained from a trusted source over an assured channel, may be used if it executes in a constrained environment without access to local system and network resources (e.g., file system, Windows registry, network connections other than to its originating host).

1.2.4. Where possible, web browsers and other mobile code enabled products shall be configured to prompt the user prior to the execution of Category 2 mobile code. Where feasible, protections against malicious Category 2 mobile code technologies shall be employed at end user systems and at enclave boundaries. The responsible CIO may grant a waiver for the use of Category 2 mobile code not obtained from a trusted source over an assured channel. If code signing is used to meet the requirement for a trusted source over an assured channel, a DoD-approved PKI code-signing certificate shall be used, if available. In the absence of a DoD-approved PKI code-signing certificate, the responsible CIO may approve alternate commercially available code signing certificates.

1.2.5. New procurement and development efforts that rely on Category 2 mobile code technologies shall include a mobile code risk mitigation strategy detailing the measures incorporated into the system development to curtail the risk posed by their use in their risk management plan, in accordance with DoDI 5200.40. The risk mitigation strategy shall be attached to the accreditation package as part of the SSAA. The responsible CIO must approve new procurement and development efforts that use Category 2 mobile code that does not meet the above restrictions (e.g., unsigned mobile code that does not execute in a constrained environment as described in paragraph 1.2.3. above, or mobile code not obtained from a trusted source over an assured channel).

1.3. Category 3

1.3.1. Category 3 mobile code technologies support limited functionality, with no capability for unmediated access to workstation, host, and remote system services and resources. Category 3 mobile code technologies may have a history of known vulnerabilities, but also support fine-grained, periodic, or continuous security safeguards.

1.3.2. Category 3 mobile code technologies pose limited risk to DoD systems. When combined with vigilance comparable to that required to keep any software system configured to resist known exploits, the use of Category 3 mobile code affords benefits that outweigh the risks.

1.3.3. Category 3 mobile code technologies may be used in DoD information systems.

1.3.4. Program Executive Officers (PEOs), Program Managers (PMs), and Executive Agents (EAs) shall develop a mobile code risk mitigation strategy as part of the risk management plan, in accordance with DoDI 5200.40. The risk mitigation strategy shall be attached to the accreditation package as part of the SSAA.

1.4. Emerging Mobile Code Technologies.

1.4.1. Emerging mobile code technologies refer to all mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet been reviewed for categorization.

1.4.2. Unless a waiver is granted under 1.4.3. below, the download and execution of mobile code using unwaivered emerging technologies shall be blocked by all means available at the enclave boundary, workstation, host, and within applications.

1.4.3. If an emerging mobile code technology is planned for use in a DoD application, the sponsoring Component will provide the DoD CIO sufficient information to evaluate and categorize the technology at least 90 days prior to initial use. If the emerging technology is not categorized within the 90-day period, the responsible CIO may grant a written waiver for its use.

1.4.4. Working through DISA, DoD will invite industry to provide a beta version of any new technology at least 90 days ahead of public release to give DoD an opportunity to evaluate and categorize it. Developers are encouraged to assist Component CIOs' efforts to sponsor categorization of emerging technologies.

2. Use of Mobile Code in E-mail.

2.1 Whenever possible, the automatic execution of all categories of mobile code in e-mail bodies and attachments shall be disabled.

2.2 Whenever possible, desktop software shall be configured to prompt the user prior to opening e-mail attachments that may contain mobile code.

Attachment

Attachment 1 to Enclosure 1
Initial Mobile Code Technology Risk Category Assignments

1. The mobile code technologies listed in paragraph 2 below are within the scope of the policy when employed in a manner satisfying the definition of mobile code found in Enclosure 2. For information and clarification, several data representation formats and technology application areas that are currently outside the scope of the policy are also identified in paragraph 3.

2. Category Assignments:

2.1.1. The following technologies are designated Category 1:

ActiveX
Windows Scripting Host, when used to execute mobile code
Unix Shell Scripts, when used as mobile code
DOS Batch Scripts, when used as mobile code

2.2.1. The following technologies are designated Category 2:

Java applets and other Java mobile code
Visual Basic for Applications (VBA)
LotusScript
PerfectScript
Postscript

2.31. The following technologies are designated Category 3:

Javascript (include Jscript and ECMAScript variants)
VBScript
Portable Document Format (PDF)
Shockwave/Flash

3. Exclusions:

3.1. Technology Exclusions. The following technologies are not presently designated as mobile code:

XML
SMIL
Quicktime
VRML (exclusive of any associated Java applets or JavaScript scripts. Applets or scripts associated with VRML worlds are subject to the policy).

3.2. Application Exclusions. The following technology application areas are outside the scope of the DoD mobile code policy.

3.2.1. Scripts and applets embedded in or linked to web pages and executed in the context of the web server. Examples of technologies in this application area include: Java servlets, Java Server Pages, CGI, Active Server Pages, CFML, PHP, SSI, server-side JavaScript, server-side LotusScript.

3.2.2. Local programs and command scripts. Examples of technologies in this application area include: binary executables, shell scripts, batch scripts, Windows Scripting Host (WSH), Perl scripts.

3.2.3. Distributed object-oriented programming systems – Examples of technologies in this area include: CORBA, DCOM. [Note: Java RMI and Java Jini technologies are included under section 3.2.1]

3.2.4. Software patches, updates, including self-extracting updates – software updates that must be invoked explicitly by the user are outside the scope of the mobile code policy. Examples of technologies in this area include: Netscape SmartUpdate, Microsoft Windows Update, Netscape web browser plug-ins, and Linux

## Enclosure 2
## Definitions

3.1. Assured Channel: A network communication link that is protected by a security protocol providing authentication and data integrity, and employs US Government approved cryptographic technologies whenever cryptographic means are utilized. The following protocols and mechanisms are sufficient to meet the requirements of authentication and data integrity protection for an assured channel: the Secret Internet Protocol Router Network (SIPRNET), Internet Protocol Security (IPSec), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Multipurpose Internet Mail Extension (S/MIME), or digital code signing using a DoD-approved PKI code signing certificate, and other systems using NSA-approved high assurance guards with link encryption methodology.

3.2. Code Signing Certificate: A public key infrastructure (PKI) certificate that can be used to digitally sign code. Such a certificate has a specially assigned attribute (referred to as the *code signing bit*) set.

3.3. Component Heads: For purposes of this policy guidance, the Component Heads include: the Office of the Secretary of Defense Principal Staff Assistants; the Secretaries of the Military Departments; the Chairman of the Joint Chiefs of Staff, the Commanders of the Combatant Commands, the Directors of the Defense Agencies; and, the Inspector General of the Department of Defense.

3.4. Enclave: For the purpose of this policy, an enclave is an information system environment that is end-to-end under the control of a single authority and has a uniform security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization (e.g., base, post, camp, or station) or a mission (e.g., Global Command and Control System (GCCS)) and may also contain multiple networks. As a standard, the enclave typically starts and ends at the premise router. For the purposes of this policy, Component domains with assured security boundaries can be treated as a single enclave

3.5. Malicious Mobile Code: Mobile code software modules designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, providing the unauthorized disclosure of information, corrupting information, denying service, or stealing resources.

3.6. Mediated Access: Access to system resources subject to the control and approval of a runtime-enforced security policy, either during execution or at the beginning of execution. A runtime-enforced security policy provides controlled access to system resources via an intermediary such as an interpreter, virtual machine, or a security manager.

3.7. Mobile Code: Mobile code is technology which allows for the creation of executable information which can be delivered to an information system and directly executed on any hardware/software architecture which has an appropriate host execution environment. This policy is focused on the receipt of executable information from sources outside the Designated Approving Authority's area of responsibility. Therefore, for the purposes of this policy, mobile code is software obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.

3.8. Mobile Code Technologies: Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, VBScript, and ActiveX).

3.9. Trusted Source: A source that is adjudged to provide reliable software code or information and whose identity can be verified by authentication. The following mechanisms are sufficient to validate the identity of a trusted source: connection via the SIPRNET, digital signature over the mobile code itself using a DoD-approved PKI code signing certificate, a commercial code signing certificate approved by the DoD CIO, or authentication of the source of the transfer by public key certificate (e.g., S/MIME, SSL server certificate from an SSL web server).

3.10. Unmediated Access: Direct use of system resources, not subject to any approval or control beyond that imposed on conventional user applications.

# FLEET NIPRNET AND SIPRNET FIREWALL POLICY

# (SHORE AND AFLOAT)

**UPDATED: 02 JULY 99**

**(Latest changes shown in red)**

# FLEET NIPRNET FIREWALL POLICY
# (SHORE AND AFLOAT)

UPDATED: 02 JULY 99

Tables 1 through 9 display services that are to be permitted or denied for all Fleet NIPRNET firewalls. If a service is not listed, the service is denied. The tables categorize services as follows:

- Table 1 - Network Infrastructure/Management Services
- Table 2 - Electronic Messaging Services
- Table 3 - Remote Access Services
- Table 4 - Network Information Discovery and Retrieval Services
- Table 5 - File Transfer Services
- Table 6 - Collaborative Services
- Table 7 - Mobile Code Services
- Table 8 - Navy Unique Services
- Table 9 - Encrypted Services

For each service, the tables:

- indicate whether the service is allowed from the NOC enterprise network out to the NIPRNET,
- indicate whether the service is allowed into the NOC enterprise network from the NIPRNET, and
- provide additional discussion regarding the use of the service between the NOC and the NIPRNET, if necessary.

| | | |
|---|---|---|
| SNMP | Allow Queries Out | Limited to status queries from internal NOC server only. |
| | Allow Replies In | Limited to status information replies from external servers in response to queries from the internal NOC server only. |
| | Discussion | The NOC and ships require the status of external networks. Ships can query status from the internal NOC server. The internal NOC server can query status of external servers.<br>SNMP should normally not be permitted through a firewall. |
| DNS | Allow Out | Restricted |
| | Allow In | Restricted |
| | Discussion | Permitted through firewall via a split DNS configuration that consists of an internal server and an external server. The external server is located on the bastion host of the firewall. The internal server resolves queries from host machines on the internal protected network(s) and forwards queries for external names to the bastion host which forwards the queries to other external DNS servers. The external server on the bastion host resolves queries from the internal server and presents a restricted DNS database to external systems. |
| NTP | Allow Out | No. |
| | Allow In | No. |
| Syslog | Allow Out | No. |
| | Allow In | No. |
| Finger | Allow Out | No. |
| | Allow In | No. |

| | | |
|---|---|---|
| ICMP | Allow In | No. |
| | Allow Out | No. |
| NIS | Allow Out | No. |
| | Allow In | No. |
| Routing | Allow Out | Yes. |
| | Allow In | No. |
| | Discussion | Due to movement of ships, limited dynamic routing is required through the firewall. This is done by redistributing OSPF information through external BGP to external systems. Inbound routing information will not be allowed. The bastion host will run the gated daemon minimized for OSPF only and augmented with MD5 authentication to the inner and outer routers.<br>By running the gated daemon on the bastion host, this arrangement increases the vulnerability of the bastion host to attacks on as yet unknown gated daemon vulnerabilities. For example, the sendmail daemon has many known (and fixed) vulnerabilities, yet new vulnerabilities are discovered every few months. |
| Netbios | Allow Out | No. |
| | Allow In | No. |
| Vines IP | Allow Out | Yes. |
| | Allow In. | Yes. |
| | Discussion | Banyan Vines IP is allowed through the firewall via packet filtering (e.g., AuthenIP) to known external servers and from known external clients. However, as this essentially tunnels Vines IP through the firewall, intruders who have attacked and compromised "trusted" external Banyan Vines networks may then be able to compromise Banyan Vines systems behind the NOC firewalls. |

**Table 1. Network Infrastructure/Management Services**

| | | |
|---|---|---|
| SMTP | Allow Out | Yes |
| | Allow In | No |
| | Discussion | All electronic smtp-based mail is proxied through a secure mail forwarder on the bastion host of the firewall. The NOC requirements are unique in that a “split email” configuration will be utilized, providing separate inbound and outbound smtp proxies so that email can still reach ships that have moved outside the firewall. |
| X.400 | Allow Out | Yes (As DMS sites come online) |
| | Allow In | Yes (As DMS sites come online) |
| | Discussion | |
| X.500 | Allow Out | Yes (As DMS sites come online) |
| | Allow In | Yes (As DMS sites come online) |
| | Discussion | |
| POP3 | Allow Out | Yes |
| | Allow In | No |
| | Discussion | Outgoing POP3 requests are proxied through the firewall to external servers. An authenticated POP3 proxy (APOP) can be used to allow inbound requests. |
| NNTP | Allow Out | Yes |
| | Allow In | No |
| | Discussion | *Outgoing NNTP requests are proxied through the firewall to external servers. Inbound requests are not allowed.* |

**Table 2. Electronic Messaging Services**

| | | |
|---|---|---|
| ‘r’ commands | Allow Out | No (REXEC, RSHELL, RLOGIN, RUSER, RHOST, RPC) |
| | Allow In | No (REXEC, RSHELL, RLOGIN, RUSER, RHOST, RPC) |
| Telnet | Allow Out | YES (Currently allowed out for legacy systems) |
| | Allow In | NO (See Discussion) |
| | Discussion | Telnet is an inherent risk for the ships unclassified LAN even when proxied with strong authentication. Current technology utilizes Web browser and E-mail. Telnet will be allowed in through the firewall only with strong authentication. Fleet Support activities that need to Telnet “IN” to assist ship with troubleshooting must coordinate with NCTAMS PAC NOC |
| X | Allow Out | No |
| | Allow In | No |
| RPC | Allow Out | No |
| | Allow In | No |
| | Discussion | This prevents the use of RPC-based applications such as MS Exchange. RPC has inherent security vulnerabilities. |
| PPTP | Allow Out | Conditional |
| | Allow In | Conditional |
| | Discussion | Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Additional mitigation steps are required. |

**Table 3. Remote Access Services**

|  |  |  |
|---|---|---|
| HTTP | Allow Out | Yes. |
|  | Allow In | No. |
|  | Discussion | Outgoing HTTP requests are proxied through the firewall to external servers.  Optionally, a filter may be integrated to prevent the accessing of objectionable sites.  Inbound requests are not allowed.  Information intended to be publicly available should be placed on a public HTTP server on the outside of the firewall. |
| SHTTP | Allow Out | Yes |
|  | Allow In | No |
|  | Discussion | SHTTP is permitted via the HTTP proxy. |
| Gopher | Allow Out | No |
|  | Allow In | No |
|  | Discussion |  |
| WAIS | Allow Out | No |
|  | Allow In | No |
| Archie | Allow Out | No |
|  | Allow In | No |

**Table 4.  Network Information Discovery and Retrieval Services**

|  |  |  |
|---|---|---|
| FTP | Allow Out | Yes (Currently allowed out for legacy systems) |
|  | Allow In. | No |
|  | Discussion | FTP is an inherent risk to the ship's unclassified LAN and is a known vulnerability. Filtering FTP to prevent the accessing of objectionable servers provides added safeguards. Information intended to be publicly available should be placed on a public FTP server on the outside of the firewall. Current technology utilizes Web browser and E-mail. FTP will be allowed in through the firewall only with strong authentication. |
| Anon FTP | Allow Out | No |
|  | Allow In | No |
| TFTP | Allow Out | No |
|  | Allow In | No |
| NFS | Allow Out | No |
|  | Allow In | No |
| Printing | Allow Out | No |
|  | Allow In | No |
| SQL*Net for Database Replication | Allow Out | Conditional |
|  | Allow In | Conditoinal |
|  | Discussion | Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Approval requires that each user must be approved, with all required IP addresses individually specified. Must be Oracle ver 8.0 or higher. Additional mitigation steps are required. |

**Table 5. File Transfer Services**

|  |  |  |
|---|---|---|
| Talk | Allow Out | No |
|  | Allow In | No |
| IRC | Allow Out | No |
|  | Allow In | No |
| Mbone | Allow Out | No |
|  | Allow In | No |
| Real Audio | Allow Out | No |
|  | Allow In | No |
| Lotus Notes for Database Replication | Allow Out | Conditional |
|  | Allow In | Conditional |
|  | Discussion | Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use.  These will not be set by default. Each user must be approved, with all required IP addresses individually specified. Additional mitigation steps are required. |

|  |  |  |
|---|---|---|
| MSNetMtg | Allow Out | No |
|  | Allow In | No. (See Discussion) |
|  | Discussion | Fleet NOCs to host NETMTG if required due to Bandwidth requirement.  Coordination required by ship and Fleet NOCs |
| Commercial ISP | Allow Out | No |
|  | Allow In | No |
|  | Discussion | Direct connectivity to any commercial ISP (AOL, COMPUSERVE, etc) will not be allowed.  PACFLT, LANTFLT, CINCUSANAVEUR, and COMUSNAVCENT Information Assurance Office is primary POC for any questions or Firewall Waiver Requests. |

**Table 6.  Collaborative Services**

| | | |
|---|---|---|
| JAVA | Allow Out | Conditional |
| | Allow In | Conditional |
| | Discussion | Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use.  These will not be set by default. Requires user(s) to have a web browser that supports restricting to trusted sites with Java only allowed at those trusted sites.  The only authorized wild card in the trusted sites list is *.mil.  All other sites must be individually approved by the local DAA/ISSM/ISSO and individuallly entered. |
| JAVA SCRIPT | Allow Out | No |
| | Allow In | No |
| ActiveX | Allow Out | No |
| | Allow In | No |

**Table 7.  Mobile Code Services**

| | | |
|---|---|---|
| JCALS | Allow Out | Yes |
| | Allow In | Yes |
| | Discussion | JCALS is permitted through the firewall on an as-needed basis through the use of a NAVSEA proxy. |
| MRMS | Allow Out | Yes |
| | Allow In | Yes |
| | Discussion | Only the “new” firewall-friendly version of MRMS is allowed via generic proxy (e.g., plug-gw). |
| MDX | Allow Out | No. |
| | Allow In | No. |
| WPS | Allow Out | No |
| | Allow In | No |
| | Discussion | WPS is used to track containment shipments of PCS and Unit moves. This program uses automated FTP/TELNET scripts. |
| TOPS | Allow Out | No |
| | Allow In | No |
| | Discussion | TOPS is used to transfer personal property information regarding PCS and Unit moves. This program uses automated FTP/TELNET scripts. |
| JASS | Allow Out | Yes |
| | Discussion | Fleet NOCs/Pierside and Regional Shore Firewalls will allow JASS connectivity via FTP outgoing port |
| STARS FL | Allow Out | Yes |
| | Discussion | Regional Shore Firewalls will be configured to allow connectivity to STARS FL system in Jacksonville |
| SALTS | Allow Out | Yes |
| | Discussion | Fleet NOCs has opened Port 16640 at Firewall and Pierside Firewalls for SALTS |
| RAD | Allow Out | Yes |

| | | |
|---|---|---|
| | Discussion | Fleet NOCs has opened Port 1101 at Firewall and Pierside Firewall to allow ships to upload CSMP to TYCOM and retrieve current ASI update |
| ISIS | Allow Out | Yes |
| | Discussion | PRNOC/Pierside Firewalls configured to allow connectivity through Port 1601 for PACFLT ships only |

**Table 8. Navy Unique Services**

|  |  |  |
|---|---|---|
| SSL | Allow Out | Yes |
|  | Allow In | Yes |
|  | Discussion |  |
| Secure Shell | Allow Out | No. |
|  | Allow In | Limited to queries from FIWC to ASIM host only. |
|  | Discussion | FIWC requires SSH to retrieve ASIM reports. Queries from FIWC shall be allowed through the firewall to the ASIM host using a generic proxy (e.g., plug-gw) and strong authentication. |
| NES traffic | Allow Out | Yes. |
|  | Allow In | Yes. |
|  | Discussion | NES encrypted traffic is allowed through the firewall via packet filtering (e.g., AuthenIP) on an as-needed basis. |

**Table 9. Encrypted Services**

# FLEET SIPRNET FIREWALL POLICY

# (SHORE AND AFLOAT)

# UPDATED: 02 JULY 99

Tables 1 through 9 display services that are to be permitted or denied for all Fleet SIPRNET firewalls. If a service is not listed, the service is denied. The tables categorize services as follows:

- Table 1 - Network Infrastructure/Management Services
- Table 2 - Electronic Messaging Services
- Table 3 - Remote Access Services
- Table 4 - Network Information Discovery and Retrieval Services
- Table 5 - File Transfer Services
- Table 6 - Collaborative Services
- Table 7 - Mobile Code Services
- Table 8 - Navy Unique Services
- Table 9 - Encrypted Services

For each service, the tables:

- indicate whether the service is allowed from the NOC enterprise network out to the SIPRNET,
- indicate whether the service is allowed into the NOC enterprise network from theSIPRNET, and
- provide additional discussion regarding the use of the service between the NOC and the SIPRNET, if necessary.

| | | |
|---|---|---|
| SNMP | Allow Queries Out | Limited to status queries from internal NOC server only. |
| | Allow Replies In | Limited to status information replies from external servers in response to queries from the internal NOC server only. |
| | Discussion | The NOC and ships require the status of external networks. Ships can query status from the internal NOC server. The internal NOC server can query status of external servers.<br>SNMP should normally not be permitted through a firewall. |
| DNS | Allow Out | Restricted |
| | Allow In | Restricted |
| | Discussion | Permitted through firewall via a split DNS configuration that consists of an internal server and an external server. The external server is located on the bastion host of the firewall. The internal server resolves queries from host machines on the internal protected network(s) and forwards queries for external names to the bastion host which forwards the queries to other external DNS servers.. The external server on the bastion host resolves queries from the internal server and presents a restricted DNS database to external systems. |
| NTP | Allow Out | No. |
| | Allow In | No. |
| Syslog | Allow Out | No. |
| | Allow In | No. |
| Finger | Allow Out | No. |
| | Allow In | No. |
| ICMP | Allow In | No. |
| | Allow Out | No. |
| NIS | Allow Out | No. |
| | Allow In | No. |

|  |  |  |
|---|---|---|
| Routing | Allow Out | Yes. |
|  | Allow In | No. |
|  | Discussion | Due to movement of ships, limited dynamic routing is required through the firewall. This is done by redistributing OSPF information through external BGP to external systems. Inbound routing information will not be allowed. The bastion host will run the gated daemon minimized for OSPF only and augmented with MD5 authentication to the inner and outer routers.<br>By running the gated daemon on the bastion host, this arrangement increases the vulnerability of the bastion host to attacks on as yet unknown gated daemon vulnerabilities. For example, the sendmail daemon has many known (and fixed) vulnerabilities, yet new vulnerabilities are discovered every few months. |
| Netbios | Allow Out | No. |
|  | Allow In | No. |
| Vines IP | Allow Out | Yes. |
|  | Allow In. | Yes. |
|  | Discussion | Banyan Vines IP is allowed through the firewall via packet filtering (e.g., AuthenIP) to known external servers and from known external clients. However, as this essentially tunnels Vines IP through the firewall, intruders who have attacked and compromised “trusted” external Banyan Vines networks may then be able to compromise Banyan Vines systems behind the NOC firewalls. |

**Table 1. Network Infrastructure/Management Services**

| | | |
|---|---|---|
| SMTP | Allow Out | Yes |
| | Allow In | No (See Discussion) |
| | Discussion | All electronic smtp-based mail is proxied through a secure mail forwarder on the bastion host of the firewall. The NOC requirements are unique in that a "split email" configuration will be utilized, providing separate inbound and outbound smtp proxies so that email can still reach ships that have moved outside the firewall. |
| X.400 | Allow Out | Yes (As DMS sites come online) |
| | Allow In | Yes (As DMS sites come online) |
| | Discussion | |
| X.500 | Allow Out | Yes (As DMS sites come online) |
| | Allow In | Yes (As DMS sites come online) |
| | Discussion | |
| POP3 | Allow Out | Yes |
| | Allow In | No |
| | Discussion | Outgoing POP3 requests are proxied through the firewall to external servers. An authenticated POP3 proxy (APOP) can be used to allow inbound requests. |
| NNTP | Allow Out | Yes. |
| | Allow In | No. |
| | Discussion | *Outgoing NNTP requests are proxied through the firewall to external servers. Inbound requests are not allowed.* |

**Table 2. Electronic Messaging Services**

| | | |
|---|---|---|
| ‘r’ commands | Allow Out | No. (REXEC, RSHELL, RLOGIN, RUSER, RHOST, RPC) |
| | Allow In | No. (REXEC, RSHELL, RLOGIN, RUSER, RHOST, RPC) |
| Telnet | Allow Out | Yes. |
| | Allow In | No |
| | Discussion | Telnet is allowed out via proxy and allowed in via a proxy with strong authentication. Fleet Support activities that need to Telnet “IN” to assist ship with troubleshooting must coordinate with NCTAMS PAC NOC |
| X | Allow Out | No. |
| | Allow In | No. |
| RPC | Allow out | Yes. |
| | Allow In | No. |
| | Discussion | *GCCS and CTAPS require RPC on the SIPRNET. RPC is allowed out through the firewall via packet filtering (e.g., AuthenIP)* |
| PPTP | Allow Out | Conditional |
| | Allow In | Conditional |
| | Discussion | Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Additional mitigation factors are required. |

**Table 3. Remote Access Services**

| | | |
|---|---|---|
| HTTP | Allow Out | Yes |
| | Allow In | No |
| | Discussion | Outgoing HTTP requests are proxied through the firewall to external servers. Optionally, a filter may be integrated to prevent the accessing of objectionable sites. Inbound requests are not allowed. Information intended to be publicly available should be placed on a public HTTP server on the outside of the firewall and will be hosted by NCTAMS PAC NOC. |
| SHTTP | Allow Out | Yes |
| | Allow In | No |
| | Discussion | SHTTP is permitted via the HTTP proxy. |
| Gopher | Allow Out | No |
| | Allow In | No |
| WAIS | Allow Out | No |
| | Allow In | No |
| Archie | Allow Out | No |
| | Allow In | No |

**Table 4. Network Information Discovery and Retrieval Services**

| | | |
|---|---|---|
| FTP | Allow Out | Yes |
| | Allow In. | No |
| | Discussion | FTP is allowed out via proxy and allowed in via a proxy with strong authentication. Optionally, a filter may be integrated to prevent the accessing of objectionable servers. Fleet Support activities coordinate with NCTAMS PAC NOC for remote login using FTP |
| Anon FTP | Allow Out | No |
| | Allow In | No |
| | Discussion | |
| TFTP | Allow Out | No |
| | Allow In | No |
| NFS | Allow Out | No |
| | Allow In | No |
| Printing | Allow Out | No |
| | Allow In | No |
| SQL*Net | Allow Out | Conditional |
| | Allow In | Conditional |
| | Discussion | Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Approval requires that each user must be approved, with all required IP addresses individually specified. Must be Oracle ver 8.0 or higher. Additional mitigation factors are required. |

**Table 5. File Transfer Services**

| | | |
|---|---|---|
| Talk | Allow Out | No. |
| | Allow In | No. |
| IRC | Allow Out | Yes |
| | Allow In | Yes |
| | Discussion | *GCCS requires IRC on the SIPRNET. IRC is allowed out through the firewall via the strongest possible security countermeasure, either a generic proxy or packet filtering.* |
| Mbone | Allow Out | No. |
| | Allow In | No. |
| Real Audio | Allow Out | Yes. |
| | Allow In | No. |
| | Discussion | *RealAudio is required for COMPASS on the SIPRNET. RealAudio is allowed out through the firewall via a proxy.* |
| Lotus Notes for Database Replication | Allow Out | Conditional |
| | Allow In | Conditional |
| | Discussion | Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Approval requires that each user must be approved, with all required IP addresses individually specified. Additional mitigation factors are required. |
| MS NetMtg | Allow Out | Yes |
| | Allow In | Yes |
| | Discussion | |

**Table 6. Collaborative Services**

| | | |
|---|---|---|
| JAVA | Allow Out | Conditional |
| | Allow In | Conditional |
| | Discussion | Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Requires user(s) to have a web browser that supports restricting to trusted sites with Java only allowed at those trusted sites. The only authorized wild card in the trusted sites list is *.mil. All other sites must be individually approved by the local DAA/ISSM/ISSO and individuallly entered. |
| JAVA SCRIPT | Allow Out | No |
| | Allow In | No |
| ActiveX | Allow Out | No |
| | Allow In | No |

**Table 7. Mobile Code Services**

| | | |
|---|---|---|
| JCALS | Allow Out | *Required*? |
| | | *Required*? |
| GCCS-M | Allow Out | Yes |
| | Allow In | Yes |
| | Discussion | GCCS-M requires specific ports and range of ports to be open to support CST Multicasting, |
| MRMS | Allow Out | No |
| | Allow In | No |
| MDX | Allow Out | Yes |
| | Allow In | No |
| | Discussion | *GCCS requires MDX and MDXNet on the SIPRNET. These services are allowed out through the firewall via a generic proxy (e.g., plug-gw) and packet filtering (e.g., AuthenIP).* |

**Table 8. Navy Unique Services**

|  |  |  |
|---|---|---|
| SSL | Allow Out | Yes |
|  | Allow In | Yes |
|  | Discussion |  |
| Secure Shell | Allow Out | No |
|  | Allow In | Limited to queries from FIWC to ASIM host only. |
|  | Discussion | FIWC requires SSH to retrieve ASIM reports. Queries from FIWC shall be allowed through the firewall to the ASIM host using a generic proxy (e.g., plug-gw) and strong authentication. |
| NES traffic | Allow Out | Yes |
|  | Allow In | Yes |
|  | Discussion | NES encrypted traffic is allowed through the firewall via packet filtering (e.g., AuthenIP) on an as-needed basis. |

## TCP AND UDP PORTS

| SERVICE | PORT | PROTOCOL | NOTES |
|---|---|---|---|
| WINS | 0 | TCP | WINDOWS INTERNET NAMING SERVICE |
| TCP PORT | 1 | TCP | TCP PORT MULTIPLEXOR |
| ECHO | 7 | UDP,TCP | ECHO SERVER |
| DISCARD | 9 | UDP,TCP | /DEV/NULL OF THE INTERNET. HARMLESS |
| SYSTAT | 11 | TCP | REPORTS ACTIVE USERS ON SYSTEM |
| NETSTAT | 15 | TCP | SEE SYSTAT |
| CHARGN | 19 | UDP,TCP | CHARACTER STREAM GENERATOR |
| FTP | 21 | TCP | FTP CONTROL CHANEL |
| SSH | 22 | TCP | SECURE SHELL |
| TELNET | 23 | TCP | ALLOWS FOR REMOTE LOGIN |
| SMTP | 25 | TCP | SIMPLE MAIL TRANSFER PROTOCOL |
| TIME | 37 | UDP,TCP | TIME OF DAY |
| WHOIS | 43 | TCP | RETURNS INFO ABOUT A SITE |
| DOMAIN | 53 | UDP,TCP | DOMAIN NAME SERVICE |
| BOOTP | 67 | UDP | PROVIDES TOO MUCH INFO ABOUT A SITE |
| TFTP | 69 | UDP | OFTEN USED TO BOOT DISKLESS WORKSTATIONS |
| GOPHER | 70 | TCP | |
| FINGER | 79 | TCP | USED TO GET INFO ON A USER OR USERS LOGGED ON TO A SYSTEM |
| HTTP | 83 | TCP | WORLD WIDE WEB |
| LINK | 87 | TCP | PRIVATE TERMINAL LINK.  USED BY HACKERS |
| KERBERO | 88 | UDP | OFFICIAL KERBERROS PORT |
| SUPDUP | 95 | TCP | SIMILAR TO TELNET. RARELY USED EXCEPT BY HACKERS |
| POP2 | 109 | TCP | POST OFFICE PROTOCOL LEVEL 2 |
| POP3 | 110 | TCP | POST OFFICE PROTOCOL LEVEL 3 |
| SUNRPC | 111 | UDP,TCP | SUN RPC PORTMAPPER |
| NNTP | 119 | TCP | NETWORK NEWS TRANSPORT PROTOCOL |
| NTP | 123 | UDP | NETWORK TIME PROTOCOL |
| NETBIOS | 137 | UDP,TCP | NETBIOS NAME SERVICE |
| NETBIOS | 138 | UDP,TCP | NETBIOS DATAGRAM SERVICE |
| NETBIOS | 139 | UDP,TCP | NETBIOS SESSION SERVICE |
| NEWS | 144 | TCP | SUN NETWORK WINDOW SYSTEM |
| SNMP | 161 | UDP | SIMPLE NETWORK MANAGEMENT PROTOCOL AGENT |
| SNMP- | 162 | UDP,TCP | SIMPLE NETWORK MANAGEMENT |

| TRAP | | | PROTOCOL SERVER |
|---|---|---|---|
| | | | |
| XDMCP | 177 | UDP | X DISPLAY MANAGER CONTROL PROTOCOL |
| GCCS-M | 389 | TCP | PORT REQUIRED FOR GCCS-M |
| EXEC | 512 | TCP | CAN BE USED WITH A REMOTE COPY PROGRAM VARIANT |
| LOGIN | 513 | TCP | REMOTE LOGIN. |
| SHELL | 514 | TCP | SIMILAR TO REXEC. VULNERABLE TO SPOOFING |
| PRINTER | 515 | TCP | BERKELEY LPR REMOTE PRINTER |
| WHO | 513 | UDP | |
| SYSLOG | 514 | UDP | IF OPEN, YOUR LOGS CAN BE ATTACKED |
| TALK | 517 | UDP | TALK SERVICE ALLOWED BETWEEN RANDOM TCP PORTS |
| NTALK | 518 | UDP | SEE TALK |
| ROUTE | 520 | UDP | IF LEFT OPEN, ROUTING TABLES ARE OPEN TO OUTSIDERS |
| GCCS-M | 522 | TCP | GCCS-M APPLICATIONS |
| UUCP | 540 | TCP | UNIX TO UNIX COPY PROTOCOL |
| UUCP | 541 | UDP,TCP | UNIX TO UNIX COPY PROTOCOL RLOGIN |
| STARS FL | 1365 | TCP | OUTGOING FTP CONNECTIVITY |
| GCCS-M | 1024 | TCP,UDP | |
| LISTENER | 1025 | TCP | USUSAL PORT FOR SYSTEM V REL 3. BLOCK INCOMING CALLS TO PORT |
| OPENWIN | 2000 | TCP | OPEN WINDOWS |
| GCCS-M | 2001 | TCP,UDP | TDBM.UNIX |
| GCCS-M | 2006 | TCP,UDP | LDBM |
| GCCS-M | 2007 | TCP,UDP | LDBM1 |
| GCCS-M | 2008 | TCP,UDP | LDBM2 |
| GCCS-M | 2009 | TCP,UDP | LDBM3 |
| GCCS-M | 2010 | TCP,UDP | ICM |
| GCCS-M | 2011 | TCP,UDP | ICM.UNIX |
| GCCS-M | 2020 | TCP,UDP | WAN |
| GCCS-M | 2021 | TCP,UDP | WAN.UNIX |
| GCCS-M | 2030 | TCP,UDP | PCM |
| GCCS-M | 2031 | TCP,UDP | PCM.UNIX |
| GCCS-M | 2040 | TCP,UDP | OCM |
| GCCS-M | 2041 | TCP,UDP | OCM.UNIX |
| GCCS-M | 2050 | TCP,UDP | BCST |
| GCCS-M | 2051 | TCP,UDP | BCST.UNIX |
| GCCS-M | 2060 | TCP,UDP | MPS |

| | | | |
|---|---|---|---|
| GCCS-M | 2061 | TCP,UDP | MPS.UNIX |
| GCCS-M | 2065 | TCP,UDP | MPR |
| GCCS-M | 2066 | TCP,UDP | MPR.UNIX |
| GCCS-M | 2070 | TCP,UDP | PRT |
| GCCS-M | 2071 | TCP,UDP | PRT.UNIX |
| GCCS-M | 2080 | TCP,UDP | ALERTD |
| GCCS-M | 2081 | TCP,UDP | ALERTD.UNIX |
| GCCS-M | 2090 | TCP,UDP | FINDER |
| GCCS-M | 2091 | TCP,UDP | FINDER.UNIX |
| GCCS-M | 2095 | TCP,UDP | IMPORTER |
| GCCS-M | 2096 | TCP,UDP | IMPORTER.UNIX |
| GCCS-M | 2100-2199 | TCP,UDP | COMM CHANNELS |
| GCCS-M | 2200-2299 | TCP,UDP | COMM BROADCASTS |
| GCCS-M | 2300 | TCP,UDP | MAP SERVER |
| GCCS-M | 2301 – 2307 | TCP,UDP | CHART, CHART 0-5 |
| GCCS-M | 2311 | TCP,UDP | CHART 6 |
| GCCS-M | 2917 | TCP,UDP | CST PROC MGR |
| GCCS-M | 2918 | TCP,UDP | CSTGDBM |
| GCCS-M | 2919 | TCP,UDP | CSTCOP |
| GCCS-M | 3031 | TCP,UDP | AMP SERVER |
| GCCS-M | 3100 | TCP,UDP | WSM0 |
| GCCS-M | 3110 | TCP,UDP | WSM1 |
| GCCS-M | 3120 | TCP,UDP | WSM2 |
| GCCS-M | 3450 | TCP,UDP | ELVIS CHART |
| GCCS-M | 3451 | TCP,UDP | ELVIS TRACKMAN |
| GCCS-M | 3452 | TCP,UDP | ELVIS GDBM |
| GCCS-M | 3456 | TCP,UDP | ELVISII CHART |
| GCCS-M | 3457 | TCP,UDP | ELVISII GDBM |
| GCCS-M | 6016 | TCP,UDP | L16DBMC |
| GCCS-M | 6017 | TCP,UDP | L16DBM1 |
| GCCS-M | 6018 | TCP,UDP | L16DBM3 |
| GCCS-M | 8010 | TCP,UDP | CSI |
| GCCS-M | 8011 | TCP,UDP | CSI1 |
| GCCS-M | 8016 | TCP,UDP | RX |
| GCCS-M | 8088 | TCP,UDP | EWCSGDBM |
| GCCS-M | 8089 | TCP,UDP | EWCSRIU |
| GCCS-M | 8090 | TCP,UDP | EWCSRIUST |
| GCCS-M | 8091 | TCP,UDP | EWCSCROSSFIX |
| GCCS-M | 8200 | TCP,UDP | ALERT1 |
| GCCS-M | 8600 | TCP,UDP | ALERT2 |

|  |  |  |  |
|---|---|---|---|
| GCCS-M | 9000 | TCP,UDP | ELVIS HTTP |
| GCCS-M | 9120 | TCP,UDP | CSTMCAST |
| GCCS-M | 9121 | TCP,UDP | CST MCAST |
| GCCS-M | 9122 | TCP,UDP | CSTMULT3 |
| GCCS-M | 9123 | TCP,UDP | CSTMULT4 |
| GCCS-M | 9124 | TCP,UDP | CSTMDPV21 |
| GCCS-M | 9125 | TCP,UDP | CSTMDPV22 |
| GCCS-M | 9126 | TCP,UDP | CSTMDPV23 |
| GCCS-M | 9127 | TCP,UDP | CSTMDPV24 |
| GCCS-M | 9128-9199 | TCP,UDP | CST |
| GCCS-M | 9200 | TCP,UDP | ELVISII HTTP |
| GCCS-M | 9202 | TCP,UDP | ELVISII VTMD |
| GCCS-M | 9204 | TCP,UDP | ELVISII TSEWSERVER |
| GCCS-M | 9206 | TCP,UDP | ELVISII SERVER |
| GCCS-M | 9500 | TCP,UDP | GFCP LAN |
| GCCS-M | 9600 | TCP,UDP | ALERT4 |
| GCCS-M | 2019 | TCP | CST POINT TO POINT |
| GCCS-M | 2020 | TCP | NETPROC (OPNOTES) |
| NFS | 2049 | UDP | NETWORK FILE SYSTEM |
| LISTEN | 2766 | TCP | SYSTEM V LISTEN. LIKE TCPMUX. |
| X11 | 6000-6XXX | TCP |  |
| IRC | 6667 | TCP | INTERNET RELAY CHAT |

# NAVFAC Intranet Style Guide

The NAVFAC Intranet Style Guide provides basic guidance to authors and editors for preparing corporate intranet pages for consistent and readable presentation of information. It is not intended to be a complete style guide for composing web pages. (For examples, see the references.) The emphasis in this guide is on simplicity. Note that intranet sites differ from Internet sites in that there is a heavier emphasis on supporting work flow processes, documentation management, and work collaboration, with more functionality and less "glitz."

A set of templates incorporating aspects of these style guidelines is available for intranet authors using MS FrontPage 98.

## Colors

The NAVFAC intranet home page colors used for graphic elements and text are blue, gold, gray, light gray, white, and black. Use of these colors on other corporate pages provides a consistent look. Use the color specifications below to match them for spot colors when working with a graphics program or HTML authoring package.

The color specifications are:

| **Color** | **R,G,B** | **Hexadecimal** |
|---|---|---|
| 🟦 | 0,0,153 | 000099 |
| 🟨 | 255,204,51 | FFCC33 |
| ▩ | 153,153,153 | 999999 |
| ⬜ | 232,232,232 | E8E8E8 |
|  | 255,255,255 | FFFFFF |
| ⬛ | 0,0,0 | 000000 |

Type should always contrast sharply with any background color. Black text on a white background provides the greatest ease of on-screen reading. Dark or patterned backgrounds can interfere with reading ease.

A "watermark" background GIF, which uses elements of the NAVFAC seal in very light gray to avoid interference with text, is available on the intranet hub server. To apply this background, specify the Hyper Text Markup Language (HTML) body tag:

**<body background="/images/watermrk.gif" bgcolor="#FFFFFF">**

## Typefaces

The NAVFAC intranet home page makes extensive use of the sans serif Verdana typeface for ease of on-screen reading. The Impact typeface is suggested for page headings. Examples are below:

Verdana body text, Size 2
**Verdana bold, Size 2**
Impact, Size 6

Graphic elements such as the header, navigation bar footer, and the NAVFAC Spotlight also make use of the Myriad typeface.

Avoid all uppercase headlines, as they are harder to read than mixed upper and lower case. (Recognizing the shape of words is important in reading, words formed with all capital letters tend to form monotonous rectangles with few distinctive shapes.)

## Page Layout and Navigation

Pages for the intranet should be designed to work at 640 by 480 screen resolution as well as at higher resolutions. It is recommended that a centered table of width 585 pixels be used to accomplish this.

High level intranet pages should also use the standard intranet header banner and footer navigation bar.

HTML providing clickable image map information and referencing the standard header banner is available on the intranet hub server at:

**/header.htm**

which references the standard header banner graphic at:

**/images/banner.gif**

HTML providing clickable image map information and referencing the standard footer navigation bar is available on the intranet hub server at:

**/footer.htm**

which references the standard footer navigation bar graphic at:

**/images/navbar.gif**

Both GIF graphics are 585 pixels wide. The imagemaps provide links to the intranet home page and basic menu pages. Within a group of pages, authors should additionally provide a link on each page to the topic or section "home".

Use vertical white space to organize hierarchies and sequences, and use horizontal white space to limit text line lengths for reading ease.

Identify the date that the page was last modified and the author or editor at the bottom of the page in italic Verdana, Size 1, just above the footer navigation bar.

## Supported Software

The NAVFAC intranet supported software suite includes:

| Category | Product(s) |
|---|---|
| **Web server** | **MS Internet Information Server** |
| **Browsers** | **MS Internet Explorer, Netscape Navigator/Communicator** |
| **HTML Authoring** | **MS FrontPage** |
| **Data Base connection** | **Cold Fusion Professional Server, Cold Fusion Studio** |

Pages should be prepared using HTML standards, avoiding browser-specific extensions, and tested with at least both Microsoft and Netscape browsers.

A set of templates incorporating aspects of these style guidelines is available for intranet authors using MS FrontPage 98.

## File Names

Although the server OS, web server, browsers, and Windows 95/Windows NT desktop OS can all handle long filenames, it is nevertheless recommended that file names used be restricted to 8 character names with 3 character extensions for the near term.

The long file names can create side effects in several ways. For example, users running browsers under DOS/Windows who save a page to disk will have the filename change to the MS-DOS filename or other assigned name, so the name will no longer match. Authors coordinating by sending pages as e-mail attachments may have problems with some e-mail applications and long filenames; sharing files on LAN drives under a network OS that is emulating MS-DOS can result in similar problems. When files are combined in a compressed file, use of certain versions of decompression software can create problems with long filenames -- if the decompression software doesn't support the long filenames and two or more filenames differ only in characters after the eighth character, the decompression of one file may overwrite a previously decompressed file. These problems will be alleviated over time.

It is also recommended that filenames be all lowercase. The NAVFAC supported operating systems are not case-sensitive with respect to filenames; however, Unix systems do have case-sensitive filenames. Keeping filenames all lowercase simplifies portability in case some of the files are moved to a Unix-based server.

## External Links

A guiding principle for the NAVFAC intranet is that we will not duplicate information available on the Internet; rather, we will reference it by linking to it.

When linking to an Internet URL, use the exit sign GIF file available from the intranet hub server at:

```
/images/exit2www.gif
```

aligned to the absolute middle of the link text, to identify to the reader that the link goes outside the intranet to the World Wide Web.

Example:

```
<a href="http://www.navy.mil/">U.S. Navy
Home Page</a><img
src="/images/exit2www.gif"
align="absmiddle">
```

U.S. Navy Home Page EXIT→W3

## Use of Frames

While there are portions of the NAVFAC intranet that appropriately use frames, the general use of frames for high level pages is discouraged.

The advantages of frames are recognized. Before employing frames, however, consider disadvantages also: frames cut up the screen into window sections that frequently require scrolling in order to view all of the frame content, and the frames advantage of making navigation transparent is also a disadvantage to many users in not providing feedback on location changes and complicating the bookmarking of locations.

## References

One very comprehensive reference is the Yale Center for Advanced Instructional Media's
Yale C/AIM WWW Style Manual, 2nd Ed. EXIT→W3

Another useful resource is Creating Killer Web Sites: The Art of Third-Generation Site Design, 2nd Ed., by David Siegel, Hayden Books, Indianapolis, 1997. A number of design tips from this book are available online starting at:
Creating Killer Websites Online Core Page EXIT→W3

*15 March 2000 carberryjj@hq.navfac.navy.mil for the vanguard team*

intranet home ■ organization ■ resources ■ announcements ■ about the intranet

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
LITTERA SCRIPTA MANET
1985

Federal Register

Thursday,
December 21, 2000

## Part II

# Architectural and Transportation Barriers Compliance Board

**36 CFR Part 1194**
**Electronic and Information Technology Accessibility Standards; Final Rule**

## ARCHITECTURAL AND TRANSPORTATION BARRIERS COMPLIANCE BOARD

## 36 CFR Part 1194

**[Docket No. 2000–01]**

**RIN 3014–AA25**

## Electronic and Information Technology Accessibility Standards

**AGENCY:** Architectural and Transportation Barriers Compliance Board.

**ACTION:** Final rule.

**SUMMARY:** The Architectural and Transportation Barriers Compliance Board (Access Board) is issuing final accessibility standards for electronic and information technology covered by section 508 of the Rehabilitation Act Amendments of 1998. Section 508 requires the Access Board to publish standards setting forth a definition of electronic and information technology and the technical and functional performance criteria necessary for such technology to comply with section 508. Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they shall ensure that the electronic and information technology allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

**DATES:** *Effective Date:* February 20, 2001.

**FOR FURTHER INFORMATION CONTACT:** Doug Wakefield, Office of Technical and Information Services, Architectural and Transportation Barriers Compliance Board, 1331 F Street, NW., suite 1000, Washington, DC 20004–1111. Telephone number (202) 272–5434 extension 139 (voice); (202) 272–5449 (TTY). Electronic mail address: wakefield@access-board.gov.

**SUPPLEMENTARY INFORMATION:**

### Availability of Copies and Electronic Access

Single copies of this publication may be obtained at no cost by calling the Access Board's automated publications order line (202) 272–5434, by pressing 2 on the telephone keypad, then 1, and requesting publication S–40 (Electronic and Information Technology Accessibility Standards Final Rule). Persons using a TTY should call (202) 272–5449. Please record a name, address, telephone number and request publication S–40. This document is available in alternate formats upon request. Persons who want a copy in an alternate format should specify the type of format (cassette tape, Braille, large print, or computer disk). This document is also available on the Board's Internet site (http://www.access-board.gov/sec508/508standards.htm).

### Background

On August 7, 1998, the President signed into law the Workforce Investment Act of 1998, which includes the Rehabilitation Act Amendments of 1998. Section 508 of the Rehabilitation Act Amendments, as amended by the Workforce Investment Act of 1998, requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they shall ensure that the electronic and information technology allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency.[1] Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities.

Section 508(a)(2)(A) requires the Architectural and Transportation Barriers Compliance Board (Access Board)[2] to publish standards setting forth a definition of electronic and information technology and the technical and functional performance criteria necessary for accessibility for such technology. If an agency determines that meeting the standards, when procuring electronic and information technology, imposes an undue burden, it must explain why meeting the standards creates an undue burden.

On March 31, 2000, the Access Board issued a notice of proposed rulemaking (NPRM) in the **Federal Register** (65 FR 17346) proposing standards for accessible electronic and information technology. The proposed standards were based on recommendations of the Electronic and Information Technology Access Advisory Committee (EITAAC). The EITAAC was convened by the Access Board in September 1998 to assist the Board in fulfilling its mandate under section 508. It was composed of 27 members including representatives of the electronic and information technology industry, organizations representing the access needs of individuals with disabilities, and other persons affected by accessibility standards for electronic and information technology. Representatives of Federal agencies, including the departments of Commerce, Defense, Education, Justice, Veterans Affairs, the Federal Communications Commission, and the General Services Administration, served as ex-officio members or observers of the EITAAC.

The public comment period for the proposed rule ended on May 30, 2000. Over 100 individuals and organizations submitted comments on the proposed standards. Comments were submitted by Federal agencies, representatives of the information technology industry, disability groups, and persons with disabilities. Approximately 35 percent of the comments came from Federal agencies. Fifteen percent came from individual companies and industry trade associations. Approximately 30 percent of the comments were from individuals with disabilities and organizations representing persons with disabilities. Eight states responded to the proposed rule and the remaining comments were from educational or research organizations.

The proposed standards covered various products, including computers, software, and electronic office

[1] Section 508 does not apply to national security systems, as that term is defined in section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).

[2] The Access Board is an independent Federal agency established by section 502 of the Rehabilitation Act (29 U.S.C. 792) whose primary mission is to promote accessibility for individuals with disabilities. The Access Board consists of 25 members. Thirteen are appointed by the President from among the public, a majority of who are required to be individuals with disabilities. The other twelve are heads of the following Federal agencies or their designees whose positions are Executive Level IV or above: The departments of Health and Human Services, Education, Transportation, Housing and Urban Development, Labor, Interior, Defense, Justice, Veterans Affairs, and Commerce; the General Services Administration; and the United States Postal Service.

equipment in the Federal sector. They provided technical criteria specific to various types of technologies and performance-based requirements, which focus on the functional capabilities of covered technologies. Specific criteria covered controls, keyboards, and keypads; software applications and operating systems (non-embedded); web-based information or applications; telecommunications functions; video or multi-media products; and information kiosks and transaction machines. Also covered was compatibility with adaptive equipment that people with disabilities commonly use for information and communication access.

## General Issues

This section of the preamble addresses general issues raised by comments filed in response to the NPRM. Individual provisions of the rule are discussed in detail under the Section-by-Section Analysis below.

### *Effective Date for the Enforcement of Section 508*

Section 508(a)(2)(A) required the Board to publish final standards for accessible electronic and information technology by February 7, 2000. Section 508(a)(3) provides that within six months after the Board publishes its standards, the Federal Acquisition Regulatory Council is required to revise the Federal Acquisition Regulation (FAR), and each Federal agency is required to revise the Federal procurement policies and directives under its control to incorporate the Board's standards.[3]

Because of the delay in publishing the standards, the proposed rule sought comment on making the standards effective six months after publication in the **Federal Register** to provide Federal agencies an opportunity to more fully understand the new standards and allow manufacturers of electronic and information technology time to ensure that their products comply with the standards before enforcement actions could be initiated. The NPRM noted that postponing the effective date of the Board's standards could not affect the right of individuals with disabilities to file complaints for electronic and information technology procured after August 7, 2000 since that right was established by the statute.

*Comment.* There was a general consensus that a delay in the effective date of the standards was warranted to provide a reasonable period of time for industry to bring their products into compliance with the Board's standards.

*Response.* On July 13, 2000, President Clinton signed into law the Military Construction Appropriations Act for Fiscal Year 2001 (Public Law 106–246) which included an amendment to section 508 of the Rehabilitation Act. Under the amendment, the effective date for the enforcement of section 508 was delayed to allow for additional time for compliance with the Board's final standards. As originally written, the enforcement provisions of section 508 would have taken effect on August 7, 2000. The amendment in Public Law 106–246 revises the enforcement date to 6 months from publication of the Board's final standards, consistent with the law's intent. As a result of the amendment, there is no need to delay the effective date of the standards. The effective date for the standards is largely an administrative provision and does not affect the date by which complaints may be filed under section 508. Complaints and lawsuits may be filed 6 months from the date of publication of these standards in the **Federal Register**.

### *Technical and Functional Performance Criteria*

Section 508 (a)(2)(A)(ii) requires the Board to develop technical and functional performance criteria necessary to implement the requirements of section 508.

*Comment.* The Information Technology Association of America (ITAA) commented that the specificity of many of the proposed provisions go beyond what may be characterized as technical and functional performance criteria. ITAA commented that the statute intended that the standards be set forth in terms of technical and functional performance criteria as opposed to technical design requirements. Performance criteria are intended to give discretion in achieving the required end result. ITAA commented that product developers, who have a broad understanding of their own products, industry standards, and future trends need this discretion to meet the requirements of section 508 and that it is impossible to predict accurately future technological advances. Design requirements, they added, inhibit development and innovation. ITAA was concerned that many of the proposed provisions would impede technological advancements because they were too specific. On the other hand, ITAA supported proposed § 1194.5, Equivalent Facilitation, because it would lessen the adverse impact of the specific requirements.

*Response.* According to administration policy, performance standards are generally to be preferred to engineering or design standards because performance standards provide the regulated parties the flexibility to achieve the regulatory objective in a more cost-effective way. The Board was given the responsibility to develop technical and functional performance criteria necessary to implement the requirements of section 508. Thus, the standards provide technical requirements as well as functional performance criteria. The standards reflect the need to be as descriptive as possible because procurement officials and others need to know when compliance with section 508 has been achieved and because the failure to meet the standards can result in an enforcement action. Several provisions, such as those regarding time-out features, have been revised in the final rule to be more performance oriented rather than specific design standards.

## Section-by-Section Analysis

This section of the preamble summarizes each of the provisions of the final rule and the comments received in response to the proposed rule. Where the provision in the final rule differs from that of the proposed rule, an explanation of the modification is provided. The text of the final rule follows this section.

## Subpart A—General

### *Section 1194.1 Purpose*

This section describes the purpose of the standards which is to implement section 508 of the Rehabilitation Act of 1973, as amended by the Workforce Investment Act of 1998. No substantive comments were received and no changes have been made to this section in the final rule.

### *Section 1194.2 Application*

This section specifies what electronic and information technology is covered by the standards. Electronic and information technology covered by section 508 must comply with each of the relevant sections of this part. For example, a computer and its software programs would be required to comply with § 1194.26, Desktop and portable computers, § 1194.21, Software applications and operating systems, and the functional performance criteria in § 1194.31. Paragraph (a) states the general statutory requirement for electronic and information technology that must comply with the standards

[3] Whenever the Access Board revises its standards, the Federal Acquisition Regulatory Council is required to revise the FAR, and each appropriate Federal agency is required to revise its procurement policies and directives within six months to incorporate the revisions.

unless doing so would result in an undue burden. The term ''undue burden'' is defined at § 1194.4 (Definitions) and is discussed in the preamble under that section.

Paragraph (a)(1) states the statutory obligation of a Federal agency to make information and data available by an alternative means when complying with the standards would result in an undue burden. For example, a Federal agency wishes to purchase a computer program that generates maps denoting regional demographics. If the agency determines that it would constitute an undue burden to purchase an accessible version of such a program, the agency would be required to make the information provided by the program available in an alternative means to users with disabilities. In addition, the requirements to make reasonable accommodations for the needs of an employee with a disability under section 501 and to provide overall program accessibility under section 504 of the Rehabilitation Act also apply.

*Comment.* The National Federation of the Blind (NFB) suggested that additional language be added that would require agencies to provide information by an alternative means at the same time the information and data are made available to others.

*Response.* This paragraph restates the general statutory requirement to provide an alternative means of providing an individual the use of the information and data. Providing individuals with information and data by an alternative means necessarily requires flexibility and will generally be dealt with on a case-by-case approach. Although, the Board agrees that information provided by an alternative means should be provided at generally the same time as the information is made available to others, the provision provides the needed flexibility to ensure that agencies can make case-by-case decisions. No substantive changes were made in the final rule.

Paragraph (a)(2) sets forth the statutory requirement for an agency to document any claim of undue burden in a procurement. Such documentation must explain in detail which provision or provisions of this rule impose an undue burden and the extent of such a burden. The agency should discuss each of the factors considered in its undue burden analysis.

*Comment.* The General Services Administration was concerned that this provision was too limiting because it only referred to products which are procured by the Federal Government and did not include products which are developed, maintained, or used. The American Council of the Blind (ACB) recommended that the requirement for documentation apply when agencies claim the lack of commercially available accessible equipment or software. The NFB commented that there should be a requirement for agencies to explain the specific alternate means to be used to provide information or data. Without such a requirement, they argued, persons with disabilities must be knowledgeable enough to inquire about an alternate means after first discovering that the product used for the information and data is not accessible. Although agencies would be expected to know in advance when products will not be accessible, persons with disabilities will not have this information until encountering the problem.

*Response.* Paragraph (a)(2) addresses the documentation of undue burden. By statute, the requirement to document an undue burden applies only to procurements. This rule does not prescribe the needed documentation of a finding of an undue burden but merely restates the statutory requirement that a finding be documented. The FAR is expected to address the needed documentation. No substantive changes have been made in the final rule.

Paragraph (b) states that procurement of products complying with this part is subject to commercial availability. The concept of commercial availability is based on existing provisions in the FAR (see 48 CFR 2.101, Definitions of Words and Terms: Commercial item).

The proposed rule provided that the standards applied to products which were available in the commercial marketplace; would be available in time to meet an agency's delivery requirements through advances in technology or performance; or were developed in response to a Government solicitation. As noted in the preamble, this language was derived from the definition for ''commercial item'' in the FAR cited above. The preamble to the proposed rule stated that the determination of commercial availability is to be applied on a provision by provision basis.

*Comment.* A number of commenters sought further clarification of this provision. Several commenters from the information technology industry and some Federal agencies were concerned that the concept of what is commercially available was more appropriately within the jurisdiction of the Federal Acquisition Regulatory Council. The American Foundation for the Blind (AFB) and the ACB wanted agencies to document their determination that a product was not commercially available similar to what is required under undue burden. The ITAA commented that commercial availability should not be applied on a provision by provision basis.

*Response.* The Board agrees that the FAR is the appropriate venue for addressing commercial availability. The Board believes that the concept of commercial availability is captured in the FAR definition of ''commercial item''.

With respect to documentation, Federal agencies may choose to document a determination that a product is not available in the commercial marketplace in anticipation of a subsequent inquiry. However, such documentation is not required by section 508.

Similar to an undue burden analysis, agencies cannot claim that a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. The final rule has been modified to clarify this application.

Paragraph (c) applies this rule to electronic and information technology developed, procured, maintained, or used by an agency directly or used by a contractor pursuant to a contract with an agency.

*Comment.* The ITAA commented that this provision conflicts with section 508. For example, they commented that if a contract required a vendor to purchase and maintain a specific computer system for the purpose of gathering and relaying certain data to an agency, the standards would apply to such a computer system even if the system would be used only by vendor employees. In addition, ITAA commented that this is not a technical and functional performance criterion, and should be addressed by the FAR.

*Response.* Consistent with section 5002(3)(C) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452) and as further discussed in section 1194.3(b) below, products used by a contractor which are incidental to a contract are not covered by this rule. For example, a Federal agency enters into a contract to have a web site developed for the agency. The contractor uses its own office system to develop the web site. The web site is required to comply with this rule since the web site is the purpose of the contract, however, the contractor's office system does not have to comply with these standards, since the equipment used to produce the web site is incidental to the contract. See section

1194.3(b) below. No changes were made to this provision in the final rule.

*Section 1194.3 General Exceptions*

This section provides general exceptions from the standards. Paragraph (a) provides an exception for telecommunications or information systems operated by agencies, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or systems which are critical to the direct fulfillment of military or intelligence missions. This exception is statutory under section 508 and is consistent with a similar exception in section 5142 of the Clinger-Cohen Act of 1996. This exception does not apply to a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). For example, software used for payroll, word processing software used for production of routine documents, ordinary telephones, copiers, fax machines, and web applications must still comply with the standards even if they are developed, procured, maintained, or used by an agency engaged in intelligence or military activities. The Board understands that the Department of Defense interprets this to mean that a computer designed to provide early missile launch detection would not be subject to these standards, nor would administrative or business systems that must be architecturally tightly coupled with a mission critical, national security system, to ensure interoperability and mission accomplishment. No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (b) provides an exception for electronic and information technology that is acquired by a contractor incidental to a Federal contract. That is, the products a contractor develops, procures, maintains, or uses which are not specified as part of a contract with a Federal agency are not required to comply with this part. For example, a consulting firm that enters into a contract with a Federal agency to produce a report is not required to procure accessible computers and word processing software to produce the report regardless of whether those products were used exclusively for the government contract or used on both government and non-government related activities since the purpose of the contract was to procure a report. Similarly, if a firm is contracted to develop a web site for a Federal agency, the web site created must be fully compliant with this part, but the firm's own web site would not be covered. No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (c) clarifies that, except as required to comply with these standards, this part does not require the installation of specific accessibility-related software or the attachment of an assistive technology device at a workstation of a Federal employee who is not an individual with a disability. Specific accessibility related software means software which has the sole function of increasing accessibility for persons with disabilities to other software programs (*e.g.,* screen magnification software). The purpose of section 508 and these standards is to build as much accessibility as is reasonably possible into general products developed, procured, maintained, or used by agencies. It is not expected that every computer will be equipped with a refreshable Braille display, or that every software program will have a built-in screen reader. Such assistive technology may be required as part of a reasonable accommodation for an employee with a disability or to provide program accessibility. To the extent that such technology is necessary, products covered by this part must not interfere with the operation of the assistive technology. No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (d) specifies that when agencies provide access to information or data to the public through electronic and information technology, agencies are not required to make equipment owned by the agency available for access and use by individuals with disabilities at a location other than that where the electronic and information technology is provided to the public, or to purchase equipment for access and use by individuals with disabilities at a location other than that where the electronic and information technology is provided to the public. For example, if an agency provides an information kiosk in a Post Office, a means to access the kiosk information for a person with a disability need not be provided in any location other than at the kiosk itself.

*Comment.* The ACB commented that where a location is not accessible, an agency must provide the information in a location that is accessible to people with disabilities.

*Response.* This paragraph restates the general statutory requirement that when agencies provide access to information or data to the public through electronic and information technology, the agencies are not required to make equipment owned by the agency available for access and use by individuals with disabilities at a location other than that where the electronic and information technology is provided to the public, or to purchase equipment for access and use by individuals with disabilities at a location other than that where the electronic and information technology is provided to the public. The accessibility of the location would be addressed under section 504 of the Rehabilitation Act or other Federal laws. No substantive changes were made in the final rule.

Paragraph (e) states that compliance with this part does not require a fundamental alteration in the nature of a product or service or its components.

*Comment.* The AFB commented that fundamental alteration is not an appropriate factor to include in this rule since the statute provides undue burden as the proper protection and allowing a fundamental alteration exemption weakens the intent of the statute and its high expectations of government. If the concept of fundamental alteration is maintained, AFB recommended that it be part of an explanation of undue burden. The Department of Commerce agreed that the inclusion of a fundamental alteration exception would negate the purpose of section 508. The Trace Research and Development Center said that the term should be defined.

The Information Technology Industry Council (ITIC) commented that the Board should expand the concept of fundamental alteration by stating that an agency should not be required to fundamentally alter the nature of a program or service that the agency offers.

*Response.* Fundamental alteration is an appropriate exception for inclusion in the standards. It means a change in the fundamental characteristic or purpose of the product or service, not merely a cosmetic or aesthetic change. For example, an agency intends to procure pocket-sized pagers for field agents for a law enforcement agency. Adding a large display to a small pager may fundamentally alter the device by significantly changing its size to such an extent that it no longer meets the purpose for which it was intended, that is to provide a communication device which fits in a shirt or jacket pocket. For some of these agents, portability of electronic equipment is a paramount concern. Generally, adding access should not change the basic purpose or characteristics of a product in a fundamental way.

*Comment.* The ITAA commented that telecommunications equipment switches, servers, and other similar ''back office'' equipment which are used for equipment maintenance and administration functions should be exempt from the standards. For example, in the case of telecommunications equipment, technicians might need to configure service databases, remove equipment panels to replace components, or run tests to verify functionality. ITAA commented that section 508 should not apply to these types of products since applying requirements to such products would have serious design and cost ramifications.

*Response.* The Board agrees and has provided an exception that products located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment are not required to comply with this part. This exception is consistent with a similar exception in the Board's guidelines under the Americans with Disabilities Act (ADA) (§ 4.1.1(5)(b) 36 CFR part 1191) and the Architectural Barriers Act (§ 4.1.2(5) exception, Uniform Federal Accessibility Standards Appendix A to 41 CFR part 101–19.6).

*Section 1194.4 Definitions*

*Accessible.* The term accessible was defined in the proposed rule in terms of compliance with the standards in this part, as is common with other accessibility standards. As proposed, if a product complies with the standards in this part, it is ''accessible''; if it does not comply, it is not accessible.

*Comment.* The Trace Research and Development Center (Trace Center) and the General Services Administration commented that the proposed definition of accessible would mean that products can be declared ''accessible'' if they are merely compatible with assistive technology and that the definition of accessible was being used as a measure of compliance. The Trace Center commented that the problem with this approach is that a product could have few or no accessibility features because it was an undue burden and still be considered accessible.

*Response.* Although the term accessible was used sparingly in the proposed rule, the Board agrees that the definition may be problematic. The term as used in the proposed rule was in fact addressing products which comply with the standards. Products covered by this part are required to comply with all applicable provisions of this part. Accordingly, the definition has been eliminated in the final rule and the term accessible is not used in the text of the final rule. A product is compliant with the requirements of section 508 of the Rehabilitation Act of 1973 (as amended by the Workforce Investment Act of 1998) by meeting all the applicable provisions of part 1194.

*Agency.* The term agency includes any Federal department or agency, including the United States Postal Service. No substantive comments were received regarding this definition and no changes have been made in the final rule.

*Alternate formats.* Certain product information is required to be made available in alternate formats to be usable by individuals with various disabilities. Consistent with the Board's Telecommunications Act Accessibility Guidelines (36 CFR part 1193), the proposed rule defined alternate formats as those formats which are usable by people with disabilities. The proposed definition noted that the formats may include Braille, ASCII text, large print, recorded audio, and accessible internet programming or coding languages, among others. ASCII refers to the American Standard Code for Information Interchange, which is an American National Standards Institute (ANSI) standard defining how computers read and write commonly used letters, numbers, punctuation marks, and other codes.

*Comment.* One commenter was concerned that the term ''accessible internet programming or coding languages'' used in the description of acceptable alternate formats was somewhat ambiguous and recommended using the term ''accessible internet formats''.

*Response.* The Board agrees that the term ''accessible internet programming or coding languages'' may be vague. In addition, as noted above, the final rule will not include the term ''accessible''. The definition for alternate formats has been modified to refer to ''electronic formats which comply with this part''. This change will permit, for instance, alternate formats to include a computer file (either on the internet or saved on a computer disk) that can be viewed by a browser and which complies with the standards for web pages. No other changes have been made to the definition in the final rule.

*Alternate methods.* The proposed rule used the term ''alternate modes'' which was defined as different means of providing information to users of products, including product documentation, such as voice, fax, relay service, TTY, internet posting, captioning, text-to-speech synthesis, and audio description.

*Comment.* One commenter suggested that ''alternate methods'' would be a better term to describe the different means of providing information. The commenter was concerned that the term alternate modes would be confused with alternate modes of operation of the product itself which does not necessarily refer to how the information is provided.

*Response.* The Board agrees that the term alternate methods is a more descriptive and less confusing term than the term alternate modes. Other than the change in terminology from alternate modes to alternate methods, no other changes have been made to the definition in the final rule.

*Assistive technology.* Assistive technology is defined as any item, piece of equipment, or system, whether acquired commercially, modified, or customized, that is commonly used to increase, maintain, or improve functional capabilities of individuals with disabilities. The definition was derived from the definition of assistive technology in the Assistive Technology Act of 1998 (29 U.S.C. 3002). The preamble to the proposed rule noted that assistive technology may include screen readers which allow persons who cannot see a visual display to either hear screen content or read the content in Braille, specialized one-handed keyboards which allow an individual to operate a computer with only one hand, and specialized audio amplifiers that allow persons with limited hearing to receive an enhanced audio signal. No substantive comments were received regarding this definition and no changes have been made in the final rule.

*Electronic and information technology.* This is the statutory term for the products covered by the standards in this part. The statute explicitly required the Board to define this term, and required the definition to be consistent with the definition of information technology in the Clinger-Cohen Act of 1996. The Board's proposed definition of information technology was identical to that in the Clinger-Cohen Act. Electronic and information technology was defined in the proposed rule to include information technology, as well as any equipment or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information.

Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Electronic and information technology includes information technology products like those listed above as well as telecommunications products (such as telephones), information kiosks and transaction machines, World Wide Web sites, multimedia, and office equipment such as copiers, and fax machines.

Consistent with the FAR,[4] the Board proposed that electronic and information technology not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

*Comment.* Several commenters recommended that the exception for HVAC control devices and medical equipment be revised in the final rule. The commenters were concerned that the exception was too broad in that it exempted equipment such as medical diagnostic equipment that they felt should be covered by the rule. In addition, the National Association of the Deaf (NAD) requested that public address systems, alarm systems, and two-way communications systems such as intercoms be expressly included as electronic and information technology.

*Response.* The exemption is consistent with existing definitions for information technology in the FAR. Public address systems, alarm systems, and two-way communications systems are already addressed by the Americans with Disabilities Act Accessibility Guidelines and will be addressed in more detail in the Board's guidelines under the Architectural Barriers Act which apply to Federal facilities. No changes have been made to the definition in the final rule.

*Information technology.* The definition of information technology is identical to that in the Clinger-Cohen Act, that is, any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. No substantive comments were received regarding this definition and no changes have been made in the final rule.

*Operable controls.* The proposed rule defined operable controls as those components of a product that require physical contact for normal operation of the device. Examples of operable controls were provided, including on/off switches, buttons, dials and knobs, mice, keypads and other input devices, copier paper trays (both for inserting paper to be copied and retrieving finished copies), coin and card slots, card readers, and similar components. The proposed rule also clarified that operable controls do not include voice-operated controls.

*Comment.* One commenter was concerned that the term paper trays was confusing and interpreted it to mean the large trays on a copier which are loaded with reams of paper for copying. The commenter suggested that the term input and output trays be used instead.

*Response.* The Board agrees that input and output trays are more descriptive. The final rule reflects this change which is intended to apply to products in their normal operation rather than when the product may be used for maintenance, repair, or occasional monitoring. For example, a user should be able to add paper to a desktop laser printer. No other changes have been made to this definition.

*Product.* The term product is used in the rule as a shorthand for electronic and information technology. No substantive comments were received regarding this definition and no changes have been made in the final rule.

*Self contained, closed products.* This term was not used in the proposed rule and is provided in the final rule as a result of the reorganization of the standards. Self contained, closed products, are those that generally have embedded software and are commonly designed in such a fashion that a user cannot easily attach or install assistive technology. These products include, but are not limited to, information kiosks and information transaction machines, copiers, printers, calculators, fax machines, and other similar types of products.

*Telecommunications.* The definition for telecommunications is consistent with the definition in the Board's Telecommunications Act Accessibility Guidelines and the definition of telecommunications in the Telecommunications Act. No substantive comments were received regarding this definition and no changes have been made in the final rule.

*TTY.* TTYs are machinery or equipment that employ interactive text based communications through the transmission of coded signals across the telephone network.

*Comment.* The Trace Center recommended adding the word ''baudot'' to the definition of TTY to clarify that the term is not meant to be broader than baudot TTYs. The NAD and other consumer groups, however, supported the Board's definition and encouraged the Board to use the same definition consistently.

*Response.* The definition for the term TTY is consistent with the definition of TTY in the Board's ADA Accessibility Guidelines and Telecommunications Act Accessibility Guidelines. No changes have been made to the definition in the final rule.

*Undue burden.* The final rule defines the term undue burden as ''significant difficulty or expense.'' In determining what is a significant difficulty or expense, each agency must consider the resources available to the program or component for which the product is being developed, maintained, used or procured. The proposed rule defined undue burden as an action that would result in significant difficulty or expense considering all agency resources available to the agency or component. The Board sought comment in the NPRM on two additional factors (identified as factor (2) and factor (3) in the preamble) for agencies to consider in assessing a determination of an undue burden. Factor (2) addressed the compatibility of an accessible product with the agency's or component's infrastructure, including security, and the difficulty of integrating the accessible product. Factor (3) concerned the functionality needed from the product and the technical difficulty involved in making the product accessible.

*Comment.* The ITAA, ITIC and the Oracle Corporation opposed the inclusion of a definition for undue burden in the final rule. Both the ITAA and the ITIC commented that defining undue burden was beyond the Board's authority. Oracle suggested that the concept of undue burden under section 508 was beyond the Board's expertise in that it was a procurement matter. The commenters were also concerned that the Board's definition was too narrow. Alternatively, if the Board was to adopt a definition for undue burden, the ITAA favored adoption of the factors associated with undue burden and

[4] 48 CFR Chapter 1, part 2, § 2.101 Definitions Information Technology (c).

undue hardship in the ADA and section 504 of the Rehabilitation Act. In particular, the ITAA recommended adoption of the ''nature and cost'' of the accommodation as a factor for consideration. ITIC favored adoption of the employment factors in title I of the ADA if the Board were to include a definition of undue burden. Both the ITAA and the ITIC also favored the adoption of factors (2) and (3) identified in the NPRM if undue burden was to be addressed in the final rule.

The remainder and majority of the commenters did not address the issue of whether the Board should adopt a definition of undue burden, but rather how to define it. At least two Federal agencies and 10 organizations representing persons with disabilities opposed the inclusion of factors (2) and (3) suggested in the NPRM. The Department of Commerce and a majority of advocacy organizations representing people with disabilities opposed factors (2) and (3) on the grounds that the factors would create a loophole for agencies to avoid compliance with section 508. The Department of Veterans Affairs opposed factor (3) as it considered that factor to be more about job assignment than undue burden. Several commenters including Sun Microsystems and Adobe Systems favored adopting factors (2) and (3) in the definition of undue burden. The Social Security Administration (SSA) and the Department of Health and Human Services, Administration for Children and Families, sought guidance as to the amount of increased cost of a product that would not constitute undue burden regardless of an agency's overall budget. Citing the example of a product that would cost 25 percent more to comply with the standards, the SSA questioned whether that would be undue or would 10 percent or 50 percent be considered undue. The General Services Administration recommended basing the financial resources available to an agency on a program basis.

*Response.* The term undue burden is based on caselaw interpreting section 504 of the Rehabilitation Act (*Southeastern Community College* v. *Davis,* 442 U.S. 397 (1979)), and has been included in agency regulations issued under section 504 since the *Davis* case. See, *e.g.,* 28 CFR 39.150. The term undue burden is also used in Title III of the ADA, 42 U.S.C. 12182(b)(2)(A)(iii). The legislative history of the ADA states that the term undue burden is derived from section 504 and the regulations thereunder, and is analogous to the term ''undue hardship'' in Title I of the ADA, which Congress defined as ''an action requiring significant difficulty or expense.'' 42 U.S.C. 12111(10)(A). See, H. Rept. 101–485, pt. 2, at 106. In the NPRM, the Board proposed adoption of ''significant difficulty or expense'' as the definition for undue burden. No changes were made to that aspect of the definition in the final rule.

Title I of the ADA lists factors to be considered in determining whether a particular action would result in an undue hardship. 42 U.S.C. 12111(10)(B)(i)–(iv). However, since title I of the ADA addresses employment and the individual accommodation of employees, not all of the factors are directly applicable to section 508 except for the financial resources of the covered facility or entity which is necessary to a determination of ''significant difficulty or expense.'' Unlike title I, section 508 requires that agencies must procure accessible electronic and information technology regardless of whether they have employees with disabilities. Requiring agencies to purchase accessible products at the outset eliminates the need for expensive retrofitting of an existing product when requested by an employee or member of the public as a reasonable accommodation at a later time.

In determining whether a particular action is an undue burden under section 508, the proposed rule provided that the resources ''available'' to an ''agency or component'' for which the product is being developed, procured, maintained, or used is an appropriate factor to consider. The language was derived from the section 504 federally conducted regulations. Those regulations limited the consideration of resources to those resources available to a ''program''. The preamble to the proposed rule noted that an agency's entire budget may not be available for purposes of complying with section 508. Many parts of agency budgets are authorized for specific purposes and are thus not available to other programs or components within the agency. The definition of undue burden has been clarified in the final rule to more clearly reflect this limitation. The provision now states that ''agency resources available to a program or component'' are to be considered in determining whether an action is an undue burden. Because available financial resources vary greatly from one agency to another, what constitutes an undue burden for a smaller agency may not be an undue burden for another, larger agency having more resources to commit to a particular procurement. Each procurement would necessarily be determined on a case-by-case basis. Because a determination of whether an action would constitute an undue burden is made on a case-by-case basis, it would be inappropriate for the Board to assess a set percentage for the increased cost of a product that would be considered an undue burden in every case.

The Board has not included factors (2) and (3) in the text of the final rule. While the Board acknowledges that these may be appropriate factors for consideration by an agency in determining whether an action is an undue burden, factors (2) and (3) were not based on established caselaw or existing regulations under section 504. Further, the Board recognizes that undue burden is determined on a case-by-case basis and that factors (2) and (3) may not apply in every determination. Agencies are not required to consider these factors and may consider other appropriate factors in their undue burden analyses.

*Comment.* Adobe Systems questioned whether a product which does not meet a provision based on a finding of undue burden, has to comply with the remaining provisions.

*Response.* The undue burden analysis is applied on a provision by provision basis. A separate undue burden analysis must be conducted and, in the case of procurements, be documented for each applicable provision.

### *Section 1194.5 Equivalent Facilitation*

This section allows the use of designs or technologies as alternatives to those prescribed in this part provided that they result in substantially equivalent or greater access to and use of a product for people with disabilities. This provision is not a ''waiver'' or ''variance'' from the requirement to provide accessibility, but a recognition that future technologies may be developed, or existing technologies could be used in a particular way, that could provide the same functional access in ways not envisioned by these standards. In evaluating whether a technology results in ''substantially equivalent or greater access,'' it is the functional outcome, not the form, which is important. For example, an information kiosk which is not accessible to a person who is blind might be made accessible by having a telephone handset that connects to a computer that responds to touch-tone commands and delivers the same information audibly. In addition, voice recognition and activation are progressing rapidly so that voice input soon may become a reasonable substitute for some or all keyboard input functions. For example, already some telephones can be dialed by voice. In effect, compliance with the performance criteria of § 1194.31 is the test for equivalent facilitation.

*Comment.* Commenters supported the Board in its recognition that accessibility may sometimes be attained through products that do not strictly comply with design standards. Several commenters supported this concept because they believed that it will result in the development of better access solutions for individuals with disabilities.

*Response.* No changes have been made to this provision in the final rule.

**Subpart B—Technical Standards (Formerly Subpart B—Accessibility Standards in the NPRM)**

*Comment.* Subpart B of the proposed rule contained four sections: § 1194.21 (General Requirements); § 1194.23 (Component Specific Standards); § 1194.25 Standards for Compatibility; and § 1194.27 (Functional Performance Criteria). The Board sought comment in the proposed rule on the organization of Subpart B in general and § 1194.21 (General Requirements), § 1194.23 (Component Specific Requirements) and § 1194.25 (Requirements for Compatibility) in particular. A number of commenters found the application of the proposed rule to be confusing due to the manner in which the rule was organized. Commenters questioned whether a specific product need only comply with the provisions under a specific heading in § 1194.23 (Component Specific Requirements) or whether they must also look to the provisions in § 1194.21 (General Requirements), as well as § 1194.25 (Compatibility). Commenters further questioned whether multiple provisions within a specific section would apply. For example, making electronic forms accessible was addressed under § 1194.23(b) (Non-embedded software applications and operating systems). Provisions for web sites were addressed separately in § 1194.23(c) (Web-based information or applications). Since electronic forms are becoming very popular on web sites, the commenters questioned whether the provisions for electronic forms under the software section should also be applied to web sites even though the section on web sites did not specifically address electronic forms. Another commenter pointed out that some provisions under § 1194.21 (General Requirements) actually addressed specific components such as touch screens, which were addressed under General Requirements in the proposed rule. Finally, other commenters noted that several provisions under § 1194.23 (Component Specific Requirements) were really compatibility concerns, such as § 1194.23(b) (Non-embedded software).

*Response.* A product must comply with the provisions under each applicable section in Subpart B. For example, a telecommunications product that has computer, software and operating systems, a keyboard, and web browser will have to comply with each of the relevant sections in Subpart B. The Board has reorganized Subpart B in the final rule as follows:

The title of Subpart B has been changed from ''Accessibility Standards'' to ''Technical Standards''.

Subpart B has been reorganized so that each section addresses specific products. For example, § 1194.21 addresses software applications, § 1194.22 addresses web-based intranet and internet information and applications, and so on. Each technical provision that applies to a product is located under that product heading. As a result, there is some redundancy in this section. However, the Board believes that this format will help clarify the application of the standards for each type of product. For example, the provision prohibiting the use of color alone to indicate an action applies not only to web page design, but also to software design and certain operating systems. In the final rule, it is addressed in § 1194.21(i) (Software applications and operating systems), § 1194.22(c) (Web-based intranet and internet information and applications), as well as § 1194.25(g) (Self contained, closed products).

The provisions contained in § 1194.21 (General Requirements), § 1194.23 (Component Specific Requirements) and § 1194.25 (Requirements for Compatibility with Assistive Technology) of the proposed rule have been moved to the new subpart B (Technical Standards) in the final rule.

Also, the provisions in the proposed rule under § 1194.27 (Functional Performance Criteria) have been redesignated as Subpart C (Functional Performance Criteria) in the final rule. Subpart C provides functional performance criteria for overall product evaluation and for technologies or components for which there is no specific provision in subpart B. The substance of each of the provisions in the final rule are discussed below.

*Section 1194.21 Software Applications and Operating Systems*

Paragraphs (a) through (l) address provisions for software applications and operating systems. Electronic and information technology products operate by following programming instructions referred to as software. Software refers to a set of logical steps (or programming instructions) that control the actions or operations of most forms of electronic and information technology products. For instance, when a pager receives a radio signal, the software embedded inside the pager determines whether the signal is a ''page'' and how it should display the information it receives. The circuitry inside the pager, including the display unit, merely follows the instructions encoded in the software. Software can be divided into two broad categories: Software that is embedded in a chip mounted in a product and non-embedded software that is loaded onto a storage device such as a hard disk and can be erased, replaced, or updated. For instance, a word processing program that is installed onto a computer's hard drive and which may be easily erased, replaced, or updated is typically ''non-embedded'' software. By contrast, the set of instructions installed on a chip inside a pager and which cannot be erased, replaced, or updated is typically embedded software. The proposed rule included provisions for non-embedded software. However, as pointed out by commenters, as technology changes, the distinction between embedded software and non-embedded software is increasingly becoming less clear. These provisions apply to all software products.

Paragraph (a) requires that when software is designed to run on a system that has a keyboard, the software shall provide a way to control features which are identifiable by text, from the keyboard. For example, if a computer program included a ''print'' command or a ''save'' command (both can be readily discerned textually), the program must provide a means of invoking these commands from the keyboard. For people who cannot accurately control a mouse, having access to the software's controls through keyboard alternatives is essential. For example, rather than pointing to a particular selection on the screen, a user may move through the choices in a dialogue box by pressing the tab key. (See § 1194.23(a)(4) and § 1194.23(b)(1) in the NPRM.)

*Comment.* The NPRM required that products must provide logical navigation among interface elements through the use of keystrokes. Commenters questioned the meaning of ''logical'' and whether the provisions, as proposed, were requiring that each system have a keyboard. Commenters were concerned that requiring that all features of every software program be accessible from a keyboard was not feasible because some programs that allow an individual to draw lines and create designs using a mouse could not be replicated with keystrokes.

*Response.* This provision applies to products which are intended to be run on a system with a keyboard. It does not require that a keyboard be added. The term ''logical navigation'' has been deleted. Only those actions which can be discerned textually are required to be executable from a keyboard. For example, most of the menu functions in common drawing programs that allow a user to open, save, size, rotate, and perform other actions on a graphic image can all be performed from the keyboard. However, providing keyboard alternatives for creating an image by selecting a paintbrush, picking a color, and actually drawing a design would be extremely difficult. Such detailed procedures require the fine level of control afforded by a pointing device (*e.g.,* a mouse) and thus cannot be discerned textually without a lengthy description. Accordingly, in the final rule, keyboard alternatives are required when the function (*e.g.,* rotate figure) or the result of performing a function (*e.g.,* save file confirmation) can be represented with words.

Paragraph (b) prohibits applications from disrupting or disabling activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer. The application programming interface refers to a standard way for programs to communicate with each other, including the operating system, and with input and output devices. For instance, the application programming interface affects how programs have to display information on a monitor or receive keyboard input via the operating system.

Many commercially available software applications and operating systems have features built-into the program that are labeled as access features. These features can typically be turned on or off by a user. Examples of these features may include, reversing the color scheme (to assist people with low vision), showing a visual prompt when an error tone is sounded (to assist persons who are deaf or hard of hearing), or providing ''sticky keys'' that allow a user to press key combinations (such as control-C) sequentially rather than simultaneously (to assist persons with dexterity disabilities). This provision prohibits software programs from disabling these features when selected. (See § 1194.23(b)(2) in the NPRM.)

*Comment.* The proposed rule only specified that software not interfere with features that affect the usability for persons with disabilities. Commenters from industry noted that the provision in the NPRM did not provide any method of identifying what features are considered access features and further stated that this provision was not achievable. These commenters pointed out that it was impossible for a software producer to be aware of all of the features in all software packages that could be considered an access feature by persons with disabilities. Sun Microsystems recommended that this provision address access features that have been developed using standard programming techniques and that have been documented by the manufacturer.

*Response.* This provision has been modified in the final rule to reference access features which have been developed and documented according to industry standards. No other changes have been made in the final rule.

Paragraph (c) requires that software applications place on the screen a visual indication of where some action may occur if a mouse click or keystroke takes place. This point on a screen indicating where an action will take place is commonly referred to as the ''focus''. This provision also requires that the focus be readable by other software programs such as screen readers used by computer users who are blind. (See § 1194.23(b)(3) in the NPRM.) No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (d) requires that software programs, through the use of program code, make information about the program's controls readable by assistive technology. Simply stated, this paragraph requires that information that can be delivered to or received from the user must be made available to assistive technology, such as screen reading software. Examples of controls would include button checkboxes, menus, and toolbars. For assistive technology to operate efficiently, it must have access to the information about a program's controls to be able to inform the user of the existence, location, and status of all controls. If an image is used to represent a program function, the information conveyed by the image must also be available in text. (See § 1194.23(b)(4) and § 1194.23(b)(5) in the NPRM.) No substantive comments were received and no changes have been made to this section, other than editorial changes.

Paragraph (e) requires that when bitmap images are used by a program to identify programmatic features, such as controls, the meaning of that image shall not change during the operation of a program. ''Bitmap images'' refer to a type of computer image commonly used in ''icons'' (*e.g.,* a small picture of a printer to activate the print command). Most screen reading programs allow users to assign text names to bitmap images. If the bitmap image changes meaning during a program's execution, the assigned identifier is no longer valid and is confusing to the user. (See § 1194.23(b)(6) in the NPRM.)

*Comment.* As proposed, this provision did not identify which images had to remain consistent during the application. The AFB commented that the provision should be modified to indicate the type of image that needs to hold a consistent meaning during the running of an application. AFB noted that this provision should apply only to those bitmaps that represent a program function, and not to all images.

*Response.* The final rule applies the provision to those images which are used to identify controls, status indicators, or other programmatic elements. No other changes have been made to this section in the final rule.

Paragraph (f) provides that software programs use the functions provided by an operating system when displaying text. The operating system is the ''core'' computer software that controls basic functions, such as receiving information from the keyboard, displaying information on the computer screen, and storing data on the hard disk. Other software programs use the standard protocols dictated by the operating system for displaying their own information or processing the output of other computer programs. When programs are written using unique schemes for writing text on the screen or use graphics, other programs such as software for assistive technology may not be able to interpret the information. This provision does not prohibit or limit an application programmer from developing unique display techniques. It requires that when a unique method is used, the text be consistently written throughout the operating system. (See § 1194.23(b)(7) in the NPRM.)

*Comment.* The proposed rule did not specify that software programs must use the functions provided by an operating system when displaying text. The NPRM required that the text would be provided through an application programming interface that supported interaction with assistive technology or that it would use system text writing tools. Commenters raised several concerns regarding this provision. Some commenters were concerned that without a recognized interface standard, there was no assurance that assistive technology would be able to access the text provided by an application. Software producers felt that the provision should not unduly restrict how programs create or display text. Baum Electronics and GW Micro pointed out that the only way to ensure that both assistive technology and applications are using a common interface, was to use the text displaying functions of the operating system.

*Response.* The Board agrees that using operating system functions is one approach that would be available to all programmers. The final rule has been modified to require that textual information be provided through the operating system functions so that it will be compatible with assistive technology. This provision does not restrict programmers from developing unique methods of displaying text on a screen. It requires that when those methods are used, the software also sends the information through the operating systems functions for displaying text.

Paragraph (g) prohibits applications from overriding user selected contrast and color selections and other individual display attributes. As described above, the operating system provides the basic functions for receiving, displaying, transmitting, or receiving information in a computer or similar product. Thus, the operating system would appear the logical choice for ''system-wide'' settings that would be respected by all computer programs on a computer. Many modern operating systems incorporate the ability to make settings system-wide as an accessibility feature. This permits, for instance, users to display all text in very large characters. Often, persons with disabilities prefer to select color, contrast, keyboard repeat rate, and keyboard sensitivity settings provided by an operating system. When an application disables these system-wide settings, accessibility is reduced. This provision allows the user to select personalized settings which cannot be disabled by software programs. (See § 1194.23(b)(9) in the NPRM.) No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (h) addresses animated text or objects. The use of animation on a screen can pose serious access problems for users of screen readers or other assistive technology applications. When important elements such as push-buttons or relevant text are animated, the user of assistive technology cannot access the application. This provision requires that in addition to the animation, an application provide the elements in a non-animated form. (See § 1194.23(b)(11)in the NPRM.) No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (i) prohibits the use of color as the single method for indicating important information. For instance, a computer program that requires a user to distinguish between otherwise identical red and blue squares for different functions (*e.g.,* printing a document versus saving a file) would not comply with this provision. Relying on color as the only method for identifying screen elements or controls poses problems, not only for people with limited or no vision, but also for those people who are color blind. This provision does not prohibit the use of color to enhance identification of important features. It does, however, require that some other method of identification, such as text labels, be combined with the use of color. (See § 1194.21(a) in the NPRM.) No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (j) requires software applications to provide users with a variety of color settings that can be used to set a range of contrast levels. (See § 1194.23(b)(8) in the NPRM.)

*Comment.* The NPRM specified a minimum number of color settings. Some commenters were concerned that the proposed provision was too specific, while others felt it was too general because it failed to measure how different levels of contrast would be produced. Several commenters suggested requiring ''a wide variety'' of color settings as recommended by the EITAAC. One commenter noted that, as proposed, the provision forbids a monochrome display. Commenters also stated that some systems do not provide users with color selection capabilities.

*Response.* The provision in the final rule is limited to those circumstances where the system allows a user to select colors. This provision requires more than just providing color choices. The available choices must also allow for different levels of contrast. Many people experience a high degree of sensitivity to bright displays. People with this condition cannot focus on a bright screen for long because they will soon be unable to distinguish individual letters. An overly bright background causes a visual ''white-out''. To alleviate this problem, the user must be able to select a softer background and appropriate foreground colors. The provision has been revised as a performance standard rather than a specific design standard by removing the requirement for 8 foreground and 8 background color selections.

Paragraph (k) limits the flashing or blinking rate of screen items. (See § 1194.21(c) in the NPRM.)

*Comment.* The Trace Center expressed concern that research supported a limit of 3 Hz, not 2 Hz as described in the NPRM. Trace suggested that the flash or blink rate avoid any flickering between (but not including) 3 Hz and 55 Hz, which is the power frequency for Europe.

*Response.* This provision is necessary because some individuals with photosensitive epilepsy can have a seizure triggered by displays which flicker or flash, particularly if the flash has a high intensity and is within certain frequency ranges. The 2 Hz limit was chosen to be consistent with proposed revisions to the ADA Accessibility Guidelines which, in turn, are being harmonized with the International Code Council (ICC)/ANSI A117 standard, ''Accessible and Usable Buildings and Facilities'', ICC/ANSI A117.1–1998 which references a 2 Hz limit. The Board agrees that an upper limit is needed, since all electrically powered equipment, even an incandescent light bulb, has a ''flicker'' due to the alternating current line voltage frequency (60 Hz in the U.S., 55 Hz in Europe). There does not appear to be any significant incidence of photosensitive seizures being induced by the line voltage frequency of ordinary lights. Therefore, the provision has been changed to prohibit flash or blink frequencies between 2 Hz and 55 Hz.

Paragraph (l) requires that people with disabilities have access to electronic forms. This section is a result of the reorganization of the final rule and is identical to section 1194.22(n) discussed below. (See § 1194.23(b)(10) in the NPRM.)

### *Section 1194.22 Web-based Intranet and Internet Information and Applications*

In the proposed rule, the Board indicated that the EITAAC had recommended that the Board's rule directly reference priority one and two checkpoints of the World Wide Web Consortiums' (W3C) Web Accessibility Initiative's (WAI) Web Content Accessibility Guidelines 1.0 (WCAG 1.0). Rather than reference the WCAG 1.0, the proposed rule and this final rule include provisions which are based generally on priority one checkpoints of the WCAG 1.0, as well as other agency documents on web accessibility and additional recommendations of the EITAAC.

*Comment.* A number of comments were received from the WAI and others expressing concern that the Board was creating an alternative set of standards that would confuse developers as to which standards should be followed. WAI was further concerned that some of the provisions and preamble language in the NPRM were inaccurate. On the other hand, a number of commenters, including the ACB and several members of the EITAAC, supported the manner in which web access issues were addressed in the proposed rule.

*Response.* The final rule does not reference the WCAG 1.0. However, the first nine provisions in § 1194.22, paragraphs (a) through (i), incorporate the exact language recommended by the WAI in its comments to the proposed rule or contain language that is not substantively different than the WCAG 1.0 and was supported in its comments.

Paragraphs (j) and (k) are meant to be consistent with similar provisions in the WCAG 1.0, however, the final rule uses language which is more consistent with enforceable regulatory language. Paragraphs (l), (m), (n), (o), and (p) are different than any comparable provision in the WCAG 1.0 and generally require a higher level of access or prescribe a more specific requirement.

The Board did not adopt or modify four of the WCAG 1.0 priority one checkpoints. These include WCAG 1.0 Checkpoint 4.1 which provides that web pages shall ‘‘[c]learly identify changes in the natural language of a document's text and any text equivalents (*e.g.,* captions).’’; WCAG 1.0 Checkpoint 14.1 which provides that web pages shall ‘‘[u]se the clearest and simplest language appropriate for a site's content.’’; WCAG 1.0 Checkpoint 1.3 which provides that ‘‘[u]ntil user agents can automatically read aloud the text equivalent of a visual track, provide an auditory description of the important information of the visual track of a multimedia presentation.’’; and WCAG 1.0 Checkpoint 6.2 which provides that web pages shall ‘‘[e]nsure that equivalents for dynamic content are updated when the dynamic content changes.’’

Section 1194.23(c)(3) of the proposed rule required that web pages alert a user when there is a change in the natural language of a page. The ‘‘natural language’’ referred to the spoken language (*e.g.,* English or French) of the web page content. The WAI pointed out that the preamble to the NPRM misinterpreted this provision. The preamble suggested that a statement such as ‘‘the following paragraph is in French’’ would meet the provision. WAI responded by noting that this was not the intent of the provision. The WCAG 1.0 recommend that web page authors embed a code or markup language in a document when the language changes so that speech synthesizers and Braille displays could adjust output accordingly.

The Trace Center advised that only two assistive technology programs could interpret such coding or markup language, Homepage Reader from IBM and PwWebspeak from Isound. These programs contain the browser, screen reading functions, and the speech synthesizer in a single highly integrated program. However, the majority of persons who are blind use a mainstream browser such as Internet Explorer or Netscape Navigator in conjunction with a screen reader. There are also several speech synthesizers in use today, but the majority of those used in the United States do not have the capability of switching to the processing of foreign language phonemes. As a result, the proposed provision that web pages alert a user when there is a change in the natural language of a page has been deleted in the final rule.

The Board also did not adopt WCAG 1.0 Checkpoint 14.1 which provides that web pages shall ‘‘[u]se the clearest and simplest language appropriate for a site's content.’’ While a worthwhile guideline, this provision was not included because it is difficult to enforce since a requirement to use the simplest language can be very subjective.

The Board did not adopt WCAG 1.0 Checkpoint 1.3 which provides that ‘‘[u]ntil user agents can automatically read aloud the text equivalent of a visual track, provide an auditory description of the important information of the visual track of a multimedia presentation.’’ Although the NPRM did not propose addressing this issue in the web section, there was a similar provision in the multi-media section of the NPRM.

The Board did not adopt WCAG 1.0 Checkpoint 6.2 which provide that web pages shall ‘‘[e]nsure that equivalents for dynamic content are updated when the dynamic content changes.’’ The NPRM had a provision that stated ‘‘web pages shall update equivalents for dynamic content whenever the dynamic content changes.’’ The WAI stated in its comments that there was no difference in meaning between the NPRM and WCAG 1.0 Checkpoint 6.2. The NPRM provision has been deleted in the final rule as the meaning of the provision is unclear.

A web site required to be accessible by section 508, would be in complete compliance if it met paragraphs (a) through (p) of these standards. It could also comply if it fully met the WCAG 1.0, priority one checkpoints and paragraphs (l), (m), (n), (o), and (p) of these standards. A Federal web site that was in compliance with these standards and that wished to meet all of the WCAG 1.0, priority one checkpoints would also have to address the WAI provision regarding using the clearest and simplest language appropriate for a site's content (WCAG 1.0 Checkpoint 14.1), the provision regarding alerting a user when there is a change in the natural language of the page (WCAG 1.0 Checkpoint 4.1), the provision regarding audio descriptions (WCAG 1.0 Checkpoint 1.3), and the provision that web pages shall ‘‘ensure that equivalents for dynamic content are updated when the dynamic content changes (WCAG 1.0 Checkpoint 6.2).

The Board has as one of its goals to take a leadership role in the development of codes and standards for accessibility. We do this by working with model code organizations and voluntary consensus standards groups that develop and periodically revise codes and standards affecting accessibility. The Board acknowledges that the WAI has been at the forefront in developing international standards for web accessibility and looks forward to working with them in the future on this vitally important area. However, the WCAG 1.0 were not developed within the regulatory enforcement framework. At the time of publication of this rule, the WAI was developing the Web Content Accessibility Guidelines 2.0. The Board plans to work closely with the WAI in the future on aspects regarding verifiability and achievability of the Web Content Accessibility Guidelines 2.0.

Paragraph (a) requires that a text equivalent for every non-text element shall be provided. As the Internet has developed, the use of photographs, images, and other multimedia has increased greatly. Most web pages are created using HTML, or ‘‘HyperText Markup Language.’’ A ‘‘page’’ in HTML is actually a computer file that includes the actual text of the web page and a series of ‘‘tags’’ that control layout, display images (which are actually separate computer files), and essentially provide all content other than text. The tags are merely signals to the browser that tell it how to display information and many tags allow web designers to include a textual description of the non-textual content arranged by the tag. The provision is necessary because assistive technology cannot describe pictures, but can convey the text information to the user. Currently, most web page authoring programs already provide a method for web designers to associate words with an image and associating text with non-textual content is easy for anyone familiar with HTML. This provision requires that when an image indicates a navigational action such as ''move to the next screen'' or ''go back to the top of the page,'' the image must be accompanied by actual text that states the purpose of the image, in other words, what the image is telling you to do. This provision also requires that when an image is used to represent page content, the image must have a text description accompanying it that explains the meaning of the image. Associating text with these images makes it possible, for someone who cannot see the screen to understand the content and navigate a web page. (See § 1194.23(c)(1) in the NPRM.)

*Comment.* In the NPRM, § 1194.23(c)(1) required text to be associated with all non-textual elements, and prescribed the use of specific techniques, such as ''alt'' and ''longdesc,'' to accomplish that requirement. WAI commented that, while the use of specific techniques was provided in WCAG 1.0 as examples of methods to use, the proposed rule was limiting the manner in which text could be associated with non-textual elements to two techniques. The result was that other approaches to providing text tags in web languages other than HTML were prohibited.

Other commenters pointed out that many images on a web page do not need text tags. They noted that some images are used to create formatting features such as spacers or borders and that requiring text identification of these images adds nothing to the comprehension of a page. These images were, in their view, textually irrelevant. One commenter suggested that this provision should address ''every non-text element'' because such features as buttons, checkboxes, or audio output were covered by other provisions in the proposed rule.

*Response.* This provision incorporates the exact language recommended by the WAI in their comments to the proposed rule. Non-text element does not mean all visible elements. The types of non-text elements requiring identification is limited to those images that provide information required for comprehension of content or to facilitate navigation. Web page authors often utilize transparent graphics for spacing. Adding text to identify these elements would produce unnecessary clutter for users of screen readers.

The Board also interprets this provision to require that when audio presentations are available on a web page, because audio is a non-textual element, text in the form of captioning must accompany the audio, to allow people who are deaf or hard of hearing to comprehend the content. (See § 1194.23(c)(1) in the NPRM.)

Paragraph (b) provides that equivalent alternatives for any multimedia presentation shall be synchronized with the presentation. This would require, for example, that if an audio portion of a multi-media production was captioned as required in paragraph (a), the captioning must be synchronized with the audio. (See § 1194.23(c)(12) and (e)(3) in the NPRM.)

*Comment.* Comments from organizations representing persons who are deaf or hard of hearing strongly supported this provision. One commenter from the technology industry raised a concern that this provision would require all live speeches broadcast on the Internet by a Federal agency to be captioned. The commenter noted that an alternative might be to provide a transcript of the speech which could be saved, reviewed, and searched.

*Response.* This provision uses language that is not substantively different than the WCAG 1.0 and was supported in the WAI comments to the proposed rule. There are new techniques for providing realtime captioning which are supported by new versions of programs like RealAudio. Providing captioning does not preclude posting a transcript of the speech for people to search or download. However, commenters preferred the realtime captioning over the delay in providing a transcript. No substantive changes have been made to this provision in the final rule.

Paragraph (c) prohibits the use of color as the single method for indicating important information on a web page. When colors are used as the sole method for identifying screen elements or controls, persons who are color blind as well as those people who are blind or have low vision may find the web page unusable. This provision does not prohibit the use of color to enhance identification of important features. It does, however, require that some other method of identification, such as text labels, must be combined with the use of color. (See § 1194.23(c)(2) in the NPRM.)

*Comment.* The WAI expressed concern that as proposed, the provision did not capture the intent of the provision as addressed in the WCAG 1.0. The intent of such a requirement, according to WAI, was to have web page designers use methods other than color to indicate emphasis such as bold text.

*Response.* This provision incorporates the exact language recommended by the WAI in their comments to the proposed rule. This provision addresses not only the problem of using color to indicate emphasized text, but also the use of color to indicate an action. For example, a web page that directs a user to ''press the green button to start'' should also identify the green button in some other fashion than simply by color.

Paragraph (d) provides that documents must be organized so they are readable without requiring browser support for style sheets. Style sheets are a relatively new technology that lets web site designers make consistent appearing web pages that can be easily updated. For instance, without style sheets, making headings appear in large font while not affecting the surrounding text requires separate tags hidden in the document to control font-size and boldface. Each heading would require a separate set of tags. Using style sheets, however, the web site designer can specify in a single tag that all headings in the document should be in large font and boldface. Because style sheets can be used to easily affect the entire appearance of a page, they are often used to enhance accessibility and this provision does not prohibit the use of style sheets. This provision requires that web pages using style sheets be able to be read accurately by browsers that do not support style sheets and by browsers that have disabled the support for style sheets. (See § 1194.23(c)(4) in the NPRM.) This requirement is based on the fact that style sheets are a relatively new technology and many users with disabilities may either not have computer software that can properly render style sheets or because they may have set their own style sheet for all web pages that they view.

*Comment.* The WAI commented that while the provision was consistent with WCAG 1.0, the preamble inaccurately noted that this provision would prohibit the use of style sheets that interfere with user defined style sheets. The WAI noted that a browser running on a user's system determines whether or not style sheets associated with pages will be downloaded.

*Response.* The WAI correctly noted that this provision does not prohibit the use of style sheets that interfere with user-defined style sheets because the use of style sheets is controlled by a user's browser. This provision uses language that is not substantively different than WCAG 1.0 and was supported in the WAI comments to the proposed rule. No substantive changes have been made to this provision in the final rule.

Paragraph (e) requires web page designers to include redundant text links for each active region of a server-side image map on their web pages. An ''image map'' is a picture (often a map) on a web page that provides different ''links'' to other web pages, depending on where a user clicks on the image. There are two basic types of image maps: ''client-side image maps'' and ''server-side image maps.'' With client-side image maps, each ''active region'' in a picture can be assigned its own ''link'' (called a URL or ''uniform resource locator'') that specifies what web page to retrieve when a portion of the picture is selected. HTML allows each active region to have its own alternative text, just like a picture can have alternative text. See § 1194.22(a). By contrast, clicking on a location of a server-side image map only specifies the coordinates within the image when the mouse was depressed—which link or URL is ultimately selected must be deciphered by the computer serving the web page. When a web page uses a server-side image map to present the user with a selection of options, browsers cannot indicate to the user the URL that will be followed when a region of the map is activated. Therefore, the redundant text link is necessary to provide access to the page for anyone not able to see or accurately click on the map. (See § 1194.23(c)(6) in the NPRM.) No substantive changes have been made to this provision in the final rule.

Paragraph (f) provides that client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape. As discussed above, there are two general categories of image maps: client-side image maps and server-side image maps. When a web browser retrieves a specific set of instructions from a client-side image map, it also receives all the information about what action will happen when a region of the map is pressed. For this reason, client-side image maps, even though graphical in nature, can display the links related to the map, in a text format which can be read with the use of assistive technology. (See § 1194.23(c)(7) in the NPRM.)

*Comment.* The WAI suggested that the final rule include an exception for those regions of a map which cannot be defined with an available geometric shape.

*Response.* This provision incorporates the exact language recommended by the WAI in their comments to the proposed rule.

Paragraphs (g) and (h) permit the use of tables, but require that the tables be coded according to the rules for developing tables of the markup language used. When tables are coded inaccurately or table codes are used for non-tabular material, some assistive technology cannot accurately read the content. Many assistive technology applications can interpret the HTML codes for tables and will most likely be updated to read the table coding of new markup languages. (See § 1194.23(c)(8–9) in the NPRM.) The Board will be developing technical assistance materials on how tables can comply with this section. In addition to these specific provisions, the technical assistance materials will address all of the provisions in this part.

*Comment.* Commenters were concerned by the preamble discussion in the NPRM which advised against the use of table tags for formatting of non-tabular material.

*Response.* The Board understands that there are currently few alternatives to the use of tables when trying to place items in predefined positions on web pages. These provisions do not prohibit the use of table codes to format non-tabular content. They require that when a table is created, appropriate coding should be used. Paragraph (g) incorporates the exact language recommended by the WAI in their comments to the proposed rule. Paragraph (h) uses language that is not substantively different than WCAG 1.0 and was supported in the WAI comments to the proposed rule. No substantive changes have been made to this provision in the final rule.

Paragraph (i) addresses the use of frames and requires that they be titled with text to identify the frame and assist in navigating the frames. ''Frames'' are a technique used by web designers to create different ''portions'' or ''frames'' of their screen that serve different functions. When a web site uses frames, often only a single frame will update with information while the other frames remain intact. Because using frames gives the user a consistent portion of the screen, they are often used for navigational toolbars for web sites. They are also often faster because only a portion of the screen is updated, instead of the entire screen. Frames can be an asset to users of screen readers and other assistive technology if the labels on the frames are explicit. Labels such as top, bottom, or left, provide few clues as to what is contained in the frame. However, labels such as ''navigation bar'' or ''main content'' are more meaningful and facilitate frame identification and navigation. (See § 1194.23(c)(10) in the NPRM.) This provision uses language that is not substantively different than WCAG 1.0. No substantive changes have been made to this provision in the final rule.

Paragraph (j) sets limits on the blink or flicker rate of screen elements. This section is a result of the reorganization of the final rule and is similar to section 1194.21(k) discussed above. (See § 1194.21(c) in the NPRM.) This provision is meant to be consistent with WCAG 1.0 Checkpoint 7.1 which provides that, ''[u]ntil user agents allow users to control flickering, avoid causing the screen to flicker.'' This provision uses language which is more consistent with enforceable regulatory language.

Paragraph (k) requires that a text-only web page shall only be provided as a last resort method for bringing a web site into compliance with the other requirements in § 1194.22. Text-only pages must contain equivalent information or functionality as the primary pages. Also, the text-only page shall be updated whenever the primary page changes. This provision is meant to be consistent with WCAG 1.0 Checkpoint 11.4 which provides that ''[i]f, after best efforts, you cannot create an accessible page, provide a link to an alternative page that uses W3C technologies, is accessible, has equivalent information (or functionality), and is updated as often as the inaccessible (original) page.''

Paragraph (l) requires that when web pages rely on special programming instructions called ''scripts'' to affect information displayed or to process user input, functional text shall be provided. It also requires that the text be readable by assistive technology such as screen reading software. Scripts are widely used by web sites as an efficient method to create faster or more secure web communications. A script is a programmatic set of instructions that is downloaded with a web page and permits the user's computer to share the processing of information with the web server. Without scripts, a user performs some action while viewing a web page, such as selecting a link or submitting a form, a message is sent back to the ''web server'', and a new web page is sent back to the user's computer. The more frequently an individual computer has to send and receive information from a web server, the greater chance there is for errors in the data, loss of speed, and possible violations of security. Also, when many users are simultaneously viewing the same web page, the demands on the web server may be huge. Scripts allow more work to be performed on the individual's computer instead of on the web server. And, the individual computer does not have to contact the web server as often. Scripts can perform very complex tasks such as those necessary to complete, verify, and submit a form and verify credit information. The advantage for the user is that many actions take place almost instantly, because processing takes place on the user's computer and because communication with the web server is often not necessary. This improves the apparent speed of a web page and makes it appear more dynamic. Currently, JavaScript, a standardized object-oriented programming language, is the most popular scripting language, although certain plug-ins (see below) support slightly different scripting languages. This provision requires web page authors to ensure that all the information placed on a screen by a script shall be available in a text form to assistive technology. (See § 1194.23(c)(11) in the NPRM.)

*Comment.* The NPRM was more specific in its application, providing that pages must be usable when scripts, applets, or other programmatic objects are turned off or are not supported. The NPRM permitted the use of an alternative accessible page. Several commenters found the proposed provision too restrictive. They noted that, as proposed, it could severely discourage innovation both for web page developers and for designers of assistive technology. It was argued that if producers of assistive technology know that a web page would never require access to scripts, there would be no incentive to develop better access to these features. It was also pointed out that discussing scripts, applets, and plug-ins in the same provision was not appropriate, because plug-ins were actual programs that run on a user's machine and do not necessarily originate on the web page. Scripts, on the other hand, are downloaded to a user's system from the web page (or an associated file) and, unlike applets or plug-ins, operate completely inside the browser without any additional software. Therefore, as scripts directly affect the actual content of a web page, the web page designer has control over designing a script but does not have control over which plug-in a user may select to process web content.

*Response.* The final rule has two separate provisions for scripts (l), and applets and plug-ins (m). Web page authors have a responsibility to provide script information in a fashion that can be read by assistive technology. When authors do not put functional text with a script, a screen reader will often read the content of the script itself in a meaningless jumble of numbers and letters. Although this jumble is text, it cannot be interpreted or used. For this reason, the provision requires that functional text, that is text that when read conveys an accurate message as to what is being displayed by the script, be provided. For instance, if a web page uses a script only to fill the contents of an HTML form with basic default values, the web page will likely comply with this requirement, as the text inserted into the form by the script may be readable by a screen reader. By contrast, if a web page uses a script to create a graphic map of menu choices when the user moves the pointer over an icon, the web site designer may be required to incorporate ''redundant text links'' that match the menu choices because functional text for each menu choice cannot be rendered to the assistive technology. Determining whether a web page meets this requirement may require careful testing by web site designers, particularly as both assistive technology and the JavaScript standard continue to evolve.

Paragraph (m) is, in part, a new provision developed in response to comments received on § 1194.23(c)(11) of the NPRM and discussed in the preceding paragraph. While most web browsers can easily read HTML and display it to the user, several private companies have developed proprietary file formats for transmitting and displaying special content, such as multimedia or very precisely defined documents. Because these file formats are proprietary, they cannot ordinarily be displayed by web browsers. To make it possible for these files to be viewed by web browsers, add-on programs or ''plug-ins'' can be downloaded and installed on the user's computer that will make it possible for their web browsers to display or play the content of the files. This provision requires that web pages which provide content such as Real Audio or PDF files, also provide a link to a plug-in that will meet the software provisions. It is very common for a web page to provide links to needed plug-ins. For example, web pages containing Real Audio almost always have a link to a source for the necessary player. This provision places a responsibility on the web page author to know that a compliant application exists, before requiring a plug-in. (See § 1194.21(c)(11) in the NPRM.)

Paragraph (n) requires that people with disabilities have access to interactive electronic forms. Electronic forms are a popular method used by many agencies to gather information or permit a person to apply for services, benefits, or employment. The 1998 Government Paperwork Elimination Act requires that Federal agencies make electronic versions of their forms available on-line when practicable and allows individuals and businesses to use electronic signatures to file these forms electronically. (See § 1194.23(b)(10) in the NPRM.) At present, the interaction between form controls and screen readers can be unpredictable, depending upon the design of the page containing these controls. Some developers place control labels and controls in different table cells; others place control labels in various locations in various distances from the controls themselves, making the response from a screen reader less than accurate many times.

*Comment.* Adobe Systems expressed concern that completing some forms requires a script or plug-in and interpreted the proposed rule as prohibiting such items. They pointed out that there are other methods of completing a form that would not require scripts or plug-ins, but those methods require the constant transfer of information between the client and server computers. Adobe noted that that method can be extremely inefficient and can pose a security risk for the individual's personal data.

*Response.* This provision does not forbid the use of scripts or plug-ins and many of the existing products support these features. If a browser does not support these features, however, paragraphs (l) and (m) require that some other method of working with the web page must be provided. As assistive technologies advance, it is anticipated that the occasions when the use of scripts and plug-ins are not supported will diminish significantly. No substantive changes have been made to this provision in the final rule.

Paragraph (o) provides that a method be used to facilitate the easy tracking of page content that provides users of assistive technology the option to skip repetitive navigation links. (See § 1194.23(c)(13) in the NPRM.) No substantive comments were received on this provision and no changes were made, other than editorial changes.

Paragraph (p) addresses the accessibility problems that can occur if a web page times-out while a user is completing a form. Web pages can be designed with scripts so that the web page disappears or ''expires'' if a response is not received within a specified amount of time. Sometimes, this technique is used for security reasons or to reduce the demands on the computer serving the web pages. A disability can have a direct impact on the speed with which a person can read, move around, or fill in a web form. For this reason, when a timed response is required, the user shall be alerted and given sufficient time to indicate that additional time is necessary. (See § 1194.21(d) in the NPRM.)

*Comment.* The proposed rule prescribed specific settings for increasing the time-out limit based on a default setting. The Board sought comment on whether a system was commercially available that would allow a user to adjust the time-out. The Board also sought information on whether the proposed provision would compromise security. Commenters responded that security would be an issue if the time-out period was extended for too long and information with personal data was left exposed. Other commenters raised the point that specifying specific multiples of the default was unrealistic and arbitrary. The Multimedia Telecommunications Association (MMTA) stated that the default was not built-into a system. Rather, it was generally something that was set by an installer or a system administrator. They also noted that in order for a user to know that more time is needed, the user must be alerted that time is about to run out.

*Response.* The provision has been revised as a performance standard rather than a specific design standard by removing the reference to a specified length of time for users to respond. The Board agrees that it would be difficult for a user to know how much more time is needed even if the time-out could be adjusted. The final rule requires only that a user be notified if a process is about to time-out and be given an opportunity to answer a prompt asking whether additional time is needed.

### *Section 1194.23 Telecommunications Products*

Paragraph (a) requires that telephone equipment shall provide a standard non-acoustic connection point for TTYs. A TTY is a device that includes a keyboard and display that is used to transmit and receive text over a telephone line using sound. Originally, TTY's used acoustic connections and the user placed the telephone handset on the TTY to transfer the sound signals between the TTY and the telephone. Handsets on many modern telephones do not fit well with many TTY acoustic couplers, allowing interference from outside noise. Individuals who use TTYs to communicate must have a non-acoustic way to connect TTYs to telephones in order to obtain clear TTY connections, such as through a direct RJ–11 connector, a 2.5 mm audio jack, or other direct connection. When a TTY is connected directly into the network, it must be possible for the acoustic pickup (microphone) to be turned off (automatically or manually) to avoid having background noise in a noisy environment mixed with the TTY signal. Since some TTY users make use of speech for outgoing communications, the microphone on/off capability must be automatic or easy to switch back and forth or a push-to-talk mode should be provided. In the Telecommunications Act Accessibility Guidelines (36 CFR Part 1193), the Board recognized that direct-connect TTYs are customer premises equipment (CPE) subject to section 255 of that Act. Since CPE is a subset of electronic and information technology, it is similarly covered by this rule. This provision was adopted from the Board's Telecommunications Act Accessibility Guidelines so that manufacturers of telecommunications and customer premises equipment covered by section 255 of the Telecommunications Act wishing to sell products to the Federal government would have a consistent set of requirements. (See § 1194.23(d)(1) in the NPRM.)

*Comment.* The MMTA commented that providing a direct connection to an analog telephone may be as simple as providing an RJ–11 jack, but that digital phones pose additional problems. It noted that most multi-line business phones operating through a PBX are digital phones. However, it also stated that TTY connectivity can be accomplished by adding an analog line similar to what would be provided for a fax machine. The MMTA further suggested that TTY manufacturers should share the burden for compatibility. Another comment suggested that the Board require the provision of a shelf and outlet for a TTY.

*Response.* In some cases, the addition of an RJ–11 connector will be the easiest solution. In other cases, the addition of a ''smart'' adapter may be necessary, similar to the dataports available on many hotel phones. Some adapters and converters have circuitry which determines the nature of the line and plug-in equipment and makes the adjustment automatically while others are manual. There is merit, however, in viewing this provision from the standpoint of the capabilities of a system as opposed to the capabilities of a single desktop unit. There may be cases in which the connection is best made at the PBX level by installing analog phone lines where necessary. The final provision has been modified to allow for either option.

With respect to the suggestion that the standards require a shelf and outlet for a TTY, these standards apply to the electronic and information technology products themselves, not the furniture they occupy. Therefore, these standards do not address auxiliary features such as shelves and electrical outlets.

Paragraph (b) requires that products providing voice communication functionality be able to support use of all commonly used cross-manufacturer, non-proprietary, standard signals used by TTYs. Some products compress or alter the audio signal in such a manner that standard signals used by TTYs are not transmitted properly, preventing successful TTY communication. This provision is consistent with the Telecommunications Act Accessibility Guidelines. (See § 1194.23(d)(2) in the NPRM.)

*Comment.* Comments from industry suggested that the Board should clarify the standard referred to as U.S. standard Baudot communications protocol. They noted that there are several standards in use in Europe. Some European products support more than one of these standards, but not the common U.S. standard. The comments said that such products would arguably comply with the provision but would not meet the intent of section 508.

*Response.* The proposed rule required that products must support all cross-manufacturer, non-proprietary protocols, not just one or two. Of course, that included the common U.S. Baudot protocol (ANSI/TIA/EIA 825). ASCII is also used, especially on dual mode TTYs, but it is less common. Compliance with international standard ITU–T Recommendation V.18 would meet this provision, but products complying with the ITU standard may not be commercially available. It is important that products and systems support the protocol used by most TTYs currently in use to avoid a disenfranchisement of the majority of persons who are deaf or hard of hearing. However, the intent of this provision is to require support of more than just Baudot or just ASCII. At present, only these two are commonly used in the U.S., but others may come into use later. While the Board does not want to disenfranchise users of current devices, neither does it want to exclude those who buy newer equipment, as long as such devices use protocols which are not proprietary and are supported by more than one manufacturer. Of course, like all the requirements of these standards, this provision is subject to commercial availability. Accordingly, the provision has been changed in the final rule by adding the phrase ''commonly used.''

Paragraph (c) provides that TTY users be able to utilize voice mail, auto-attendant, and interactive voice response telecommunications systems. Voice mail systems are available which allow TTY users to retrieve and leave TTY messages. This provision does not require that phone systems have voice to text conversion capabilities. It requires that TTY users can retrieve and leave TTY messages and utilize interactive systems. (See § 1194.23(d)(3) in the NPRM.)

*Comment.* One commenter suggested that the Board encourage developers to build-in direct TTY decoding so that external TTYs are not required. For example, if an employee had voice mail with TTY functionality built-in, that employee would be able to read TTY messages through the computer system directly, without needing to attach an external TTY. The commenter noted that this would be beneficial to Federal agencies having telephone communication with members of the public who have speech or hearing disabilities. The agency could then have direct communication rather than being required to use an external TTY device or utilizing a relay service. Another said telecommunications systems should be required to have TTY decoding capability built-in, to the maximum extent possible. Another commenter pointed out that voice mail, voice response, and interactive systems depend on DTMF ''touch tones'' for operation and that many TTYs do not provide this function. Also, one commenter noted that automatic speech recognition (ASR) is not yet mature, but requested that a requirement for ASR be reviewed every two years to determine the feasibility of including such capabilities in products based on the rapid change of technology.

*Response.* This provision requires that voice mail, auto-attendant, and interactive voice response systems be usable with TTYs. It is desirable that computers have built-in TTY capability and there are currently systems which can add such functionality to computers. This provision is a performance requirement and the Board does not feel it would be useful to be more specific at this time. The current problems with voice mail and voice response systems are not necessarily susceptible to a single solution and there are several ways to comply, including voice recognition in some cases, depending on the system. Many voice mail systems could record a TTY message, just like a voice message, but the outgoing message needs to include a TTY prompt letting TTY users to know when to start keying. A requirement for a quick response to menu choices is the most frequently reported barrier for relay users. The ability to ''opt out'' of a menu and connect with an operator or transfer to a TTY system are also ways to make these services available and usable without highly sophisticated decoding technology.

Paragraph (d) addresses access problems that can arise when telecommunications systems require a response from a user within a certain time. Due to the nature of the equipment, users of TTYs may need additional time to read and respond to menus and messages. This provision is identical to section 1194.22(p) discussed above. (See § 1194.21(d)(4) in the NPRM.)

*Comment.* The proposed rule prescribed specific settings for increasing the time-out limit based on a default setting. Commenters raised the point that specifying specific multiples of the default was unrealistic and arbitrary. The MMTA stated that the default was not built-into a system. Rather it was generally something that was set by an installer or a system administrator. It also noted that in order for users to know that more time is needed, they must be alerted that time is about to run out.

*Response.* The provision has been changed to a performance standard rather than a specific design standard by removing the reference to a specified length of time for users to respond. The Board agrees that it would be difficult for a user to know how much more time is needed even if the time-out could be adjusted. The final rule requires only that a user be notified if a process is about to time-out and be given an opportunity to answer a prompt asking whether additional time is needed.

Paragraph (e) requires that functions such as caller identification must be accessible for users of TTYs, and for users who cannot see displays. (See § 1194.23(d)(5) in the NPRM.)

*Comment.* One commenter thought the reference to telecommunications relay services in the NPRM implied that caller identification information must somehow be transmitted directly to the end-user.

*Response.* Since the end-users in a telecommunications relay service are not directly connected, passing along caller identification information is not commonly done, therefore, the reference to relay services has been deleted to avoid confusion.

Paragraph (f) requires products to be equipped with volume control that provides an adjustable amplification up to a minimum of 20 dB of gain. If a volume adjustment is provided that allows a user to set the level anywhere from 0 to the upper requirement of 20 dB, there is no need to specify a lower limit. If a stepped volume control is provided, one of the intermediate levels must provide 12 dB of gain. The gain applies to the voice output. (See § 1194.23(d)(6) in the NPRM.)

*Comment.* Several commenters supported the provision for a 20 dB gain, but some supported a 25 dB requirement, pointing out that many persons who are hard of hearing need more than 20 dB amplification. Others urged the Board to adopt the current Federal Communications Commission's (FCC) requirement for a minimum of 12 dB and a maximum of 18 dB. Some commenters said amplifying a poor quality signal would not be useful and that the amplification may itself introduce distortion.

*Response.* The proposed level of amplification was different from that required under the FCC regulations implementing the Hearing Aid Compatibility Act (47 CFR 68.317 (a)). The FCC requires volume control that provides, through the receiver in the handset or headset of the telephone, 12 dB of gain minimum and up to 18 dB of gain maximum, when measured in terms of Receive Objective Loudness Rating.

The Board's provision is consistent with the 1998 ANSI A117.1 document, ''Accessible and Usable Buildings and Facilities.'' ANSI is the voluntary standard-setting body which issues accessibility standards used by the nation's model building codes. The Board has issued a separate NPRM to harmonize the existing ADAAG provision with the ANSI standard. The FCC originally selected its requirement to be consistent with the ADA Accessibility Guidelines now being proposed for amendment. This provision is consistent with the proposed ADA and Architectural Barriers Act Accessibility Guidelines and the Telecommunications Act Accessibility Guidelines. No changes were made to this provision in the final rule.

Paragraph (g) requires that an automatic reset be installed on any telephone that allows the user to adjust the volume higher than the normal level. This is a safety feature to protect people from suffering damage to their hearing if they accidentally answer a telephone with the amplification turned too high. (See § 1194.23(d)(7) in the NPRM.)

*Comment.* Most commenters supported the provision for an automatic reset. One commenter said the reset would be a problem for an individual user who would be required to constantly readjust his or her telephone to a usable level.

*Response.* The provision is adopted from the ADA Accessibility Guidelines, where it applies to public phones used by many people. The FCC's Part 68 rules require an automatic reset when the phone is hung up if the volume exceeds 18 dB gain. To provide the ability to override the reset function would require a waiver from the FCC since the standards require a 20 dB gain. No changes have been made to this section in the final rule.

Paragraph (h) requires telephones, or other products that provide auditory output by an audio transducer normally held up to the ear, to provide a means for effective wireless coupling to hearing aids. Many hearing aids incorporate ''T-coils'' that generate sounds based on magnetic signals received from earpieces that can generate the appropriate magnetic field. Generally, this provision means the earpiece generates sufficient magnetic field strength to induce an appropriate field in a hearing aid T-coil. The output in this case is the direct voice output of the transmission source, not the ''machine language'' such as tonal codes transmitted by TTYs. For example, a telephone must generate a magnetic output so that the hearing aid equipped with a T-coil can accurately receive the message. This provision is consistent with the Telecommunications Act Accessibility Guidelines. (See § 1194.23(d)(8) in the NPRM.) No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (i) requires that interference to hearing technologies be reduced to the lowest possible level that allows a user of hearing technologies to utilize a telecommunications product. Individuals who are hard of hearing use hearing aids and other assistive listening devices, but they cannot be used if products introduce noise into the listening aids because of electromagnetic interference. (See § 1194.23(d)(9) in the NPRM.)

*Comment.* The American National Standards Institutes (ANSI) is developing methods of measurement and defining the limits for hearing aid compatibility and accessibility to wireless telecommunications. At the time of the proposed rule, the ANSI C63.19 ANSI/IEEE Standard for Hearing Aid Compatibility with Wireless Devices was not completed. The NPRM noted that the Board may ultimately incorporate the standard when it is completed. Several commenters recommended referencing the work of the ANSI committee.

*Response.* The ANSI committee has recently completed its work. No changes have been made to this provision in the final rule and the provision continues to be a performance standard rather than a specific design standard. However, compliance with the ANSI C63.19 ANSI/IEEE Standard for Hearing Aid Compatibility with Wireless Devices would meet this provision.

Paragraph (j) provides that all products that act as a transport or conduit for information or communication shall pass all codes, translation protocols, formats, or any other information necessary to provide information or communication in a usable format. In particular, signal compression technologies shall not remove information needed for access or shall restore it upon decompression. Some transmissions include codes or tags embedded in ''unused'' portions of the signal to provide accessibility. For example, closed captioning information is usually included in portions of a video signal not seen by users without decoders. This section prohibits products from stripping out such information or requires the information to be restored at the end point. (See § 1194.25(a) in the NPRM.) No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (k) addresses controls that require some physical force to activate. It is the application of force to these controls that distinguishes them from touch sensitive controls where the mere presence of a hand or finger is detected and reacted to by the product. (See § 1194.23(a) in the NPRM.)

*Comment.* As proposed, this provision addressed mechanically operated controls, keyboard, and keypads. Commenters were concerned that the provisions were too general. Some commenters said that it was possible to interpret this section as applying to touchscreens, and that making touchscreen controls compliant with these provisions was not possible. Commenters also raised the question of whether the proposed standards would require every product to have a keyboard.

*Response.* This provision has been amended to clarify its application to mechanically operated controls. The provision only applies to products which have mechanically operated controls or keys and therefore does not require every product to have a keyboard. This provision was not intended to apply to touchscreens as touchscreens do not have mechanically operated controls.

Paragraph (k)(1) provides that mechanically operated controls and keys shall be tactilely discernible without activating the controls or keys. Tactilely discernible means that individual keys can be located and distinguished from adjacent keys by touch. To comply with this provision, controls that must be touched to activate, must be distinguishable from each other. This can be accomplished by using various shapes, spacing, or tactile markings. Because touch is necessary to discern tactile features, this provision provides that the control should not be activated by mere contact. For example, the standard desktop computer keyboard would meet this provision because the tactile mark on the ''j'' and ''f'' keys permits a user to locate all other keys tactilely. The geographic spacing of the function, ''numpad'' and cursor keys make them easy to locate by touch. In addition, most keyboards require some pressure before they transmit a keystroke. Conversely, ''capacitance'' keyboards that react as soon as they are touched and have no raised marks or actual keys would not meet this provision. A ''membrane'' keypad with keys that must be pressed can be made tactilely discernible by separating keys with raised ridges so that individual keys can be distinguished by touch. (See § 1194.23(a)(1) in the NPRM.) No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (k)(2) provides that mechanically operated controls shall be accessible to persons with limited dexterity. Individuals with tremor, cerebral palsy, paralysis, arthritis, or artificial hands may have difficulty operating systems which require fine motor control, assume a steady hand, or require two hands or fingers to be used simultaneously for operation. Individuals with high spinal cord injuries, arthritis, and other conditions may have difficulty operating controls which require significant strength. The provision limits the force required to five pounds and is based on § 4.27.4 of the ADA Accessibility Guidelines and is consistent with the Telecommunications Act Accessibility Guidelines. (See § 1194.23(a)(3) in the NPRM.)

*Comment.* The ITIC was concerned about requiring that all controls be easily activated. They pointed out that on many pieces of equipment the on/off switch is purposely set so that it is hard to activate. This is done to prevent accidental shut-down of equipment such as with a network server. They felt it was unreasonable to require changing that type of control.

*Response.* The Board has addressed this issue by adding § 1194.3(f) which exempts such controls from these standards. The on/off switch on a network server for example, would be operated only when maintenance of the equipment was required and would not be for normal operation. No changes have been made to this section in the final rule.

Paragraph (k)(3) establishes provisions for key repeat rate where an adjustable keyboard repeat rate is supported. It requires that the keyboard delay before repeat shall be adjustable to at least two seconds per character. (See § 1194.23(a)(5) in the NPRM.) No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (k)(4) provides that the status of toggle controls such as the ''caps lock'' or ''scroll lock'' keys be determined by both visual means and by touch or sound. For example, adding audio patterns such as ascending and descending pitch tones that indicate when a control is turned on or off would alleviate the problem of a person who is blind inadvertently pressing the locking or toggle controls. Also, buttons which remain depressed when activated or switches with distinct positions would meet this provision. (See § 1194.23(a)(2) in the NPRM.) No substantive comments were received and no changes have been made to this section in the final rule.

### *Section 1194.24 Video and Multimedia Products*

Paragraph (a) requires that television displays 13 inches and larger, and computer equipment that includes television receiver or display circuitry be equipped with the capacity to decode and display captioning for audio material. (See § 1194.23(e)(1) in the NPRM.)

*Comment.* Commenters supported this provision in general, but provided suggestions for clarification. They noted that the FCC defines ''television receiver'' as a device that can receive and display signals from broadcast, satellite, cable transmission, or other similar transmission sources. The commenters recommended that the provision should also address television monitors that are used with video cassette recorders (VCRs), digital video disks (DVDs), or direct video input, but do not include tuners. These non-receiver displays are commonly used throughout the government and in educational institutions and therefore, should have the capability to decode closed captions. According to commenters, the provision should reference analog television's ''line-21, NTSC'' or ''EIA–608'' caption data decoding capabilities. Many DVD presentations already include line-21 captions and commenters expressed frustration with their inability to see these captions on their desktop or laptop computers. Commenters noted that subtitles are not a substitute for captions, as captions convey more than just dialog. One commenter stated that the provision should apply to screens 10 inches or larger; while another said that digital television (DTV) will allow usable captions on smaller screens and the Board should reference the digital captioning standard EIA–708.

*Response.* This provision has been clarified to cover all television displays, not just those defined as a receiver under the FCC definition. The 13-inch display size was chosen because it is consistent with the Television Decoder Circuitry Act of 1990. The term ''analog'' added to this provision clarifies the application of the provision.

At the time of the issuance of the NPRM, the FCC was considering a rule on digital television, but had not completed its rulemaking. On July 21, 2000, the FCC issued an order on decoder circuitry standards for DTV. That standard will take effect on July 1, 2002. Devices covered under the FCC rules include DTV sets with integrated ''widescreen'' displays measuring at least 7.8 inches vertically, DTV sets with conventional displays measuring at least 13 inches vertically, and stand-alone DTV tuners, whether or not they are marketed with display screens. The provision in the final rule has been changed to reflect the FCC regulation.

Paragraph (b) requires that television tuners, including tuner cards for use in computers, have the ability to handle a secondary audio track used for audio description of visual material. The secondary audio channel is commonly used for audio description. An ''audio description'' is a verbal description of the visual content of a presentation. Audio descriptions are important for persons who are blind or who have low vision because they provide a description of the visual content of a presentation synchronized with verbal information. (See § 1194.23(e)(2) in the NPRM.) No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (c) requires the captioning of audio material in certain multimedia presentations. (See § 1194.23(e)(3) in the NPRM.)

*Comment.* The NPRM limited the provision for captioning to productions that were procured or developed for repeated showings to audiences that may include people who are deaf or hard of hearing. Commenters were concerned that agencies would avoid this provision by saying that they did not anticipate having members of the audience who were deaf or hard of hearing. Commenters noted that in many instances providing an interpreter may not be a suitable alternative. They also pointed out that subtitles are not an effective substitute for captioning multimedia presentations because subtitles do not display the environmental sounds, descriptions of music, or additional text that conveys a richer content than mere translation of the spoken dialogue.

*Response.* As proposed, the provision was intended to require captioning whenever the audience might include a person who was deaf or hard of hearing. The final rule has been modified to require that all training and informational video and multimedia presentations that contain speech or other audio information necessary for the comprehension of the content and which supports an agency's mission, shall be open or closed captioned regardless of the anticipated audience. This provision would not require that a videotape recorded by a field investigator to document a safety violation be captioned or audio described, for example. On the other hand, if such a videotape were subsequently used as part of a training or informational presentation, it would have to be captioned and audio described. A video of a retirement celebration would not be in support of an agency's mission and would thus not be required to be captioned. Also, this provision applies only to video and multimedia presentations which contain speech or other audio information necessary for the comprehension of the content. A video that is not narrated would not be required to be captioned since it does not contain speech. The NPRM asked a question about the availability of software products that could be used to provide captioning or description to multimedia computer presentations. Information supplied by commenters suggests such products are readily available.

Paragraph (d) requires that certain multimedia presentations provide an audio description of visual material. (See § 1194.23(e)(4) in the NPRM.)

*Comment.* The proposed rule limited the provision for audio description to productions that were procured or developed for repeated showings to audiences that may include people who are blind or who have low vision. Similar to (c) above, commenters were concerned that agencies may use the limitation to avoid providing the audio description.

*Response.* This provision has been modified to require audio description regardless of the anticipated audience. The final rule has been modified to require that all training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain visual information necessary for the comprehension of the content, shall be audio described. A video or multimedia presentation that does not support an agency's mission would not be required to be audio described. Also, this provision applies only to videos or multimedia presentations which contain visual information necessary for the comprehension of the content. A ''talking heads'' video does not generally contain visual information necessary for the comprehension of the content and would therefore not be required to be audio described.

Paragraph (e) provides that the captioning and audio description required in (c) and (d) above must be user selectable unless permanent. (See § 1194.23(e)(5) in the NPRM.)

*Comment.* The National Center for Accessible Media (NCAM) at public television station WGBH indicated that unlike captioning, audio descriptions can only be hidden and then activated on request on broadcast or cablecast video. The videotape format VHS commonly used by consumers and many companies cannot encode audio description for later activation like closed captions. Videos in the VHS format must have their descriptions permanently recorded as part of the main audio program. As a result, the audio descriptions on VHS cannot be turned off. As a solution, NCAM suggested that it may be desirable to have a separate videotape available that was not described, along with a described version to allow a user to choose which version they wish to present. Unlike the VHS format, CD–ROMs, DVDs and other multimedia can support alternate audio channels for descriptions (or alternate languages). The means of choosing those alternate tracks varies by the medium, but usually involves selection from an on-screen menu. Those menus must be made audible or otherwise readily selectable so that people who are blind or visually impaired can independently select and gain access to those audio descriptions.

*Response.* While the displaying of captioning is user selectable, there may be instances where the audio description would be considered permanent. The provision provides that when permanent, the user selectability provision does not apply. No changes have been made to this section in the final rule.

*Section 1194.25 Self Contained, Closed Products*

Sections 1194.25 (a) through (j) apply to those products that generally have embedded software and are commonly designed in such a fashion that a user cannot easily attach or install assistive technology. This section is a result of the reorganization of the final rule. In some instances, a personal computer with a touch-screen will be enclosed in a display and used as an ''information kiosk''. Self contained, closed products include, but are not limited to, information kiosks and information transaction machines, copiers, printers, calculators, fax machines, and other similar types of products. A definition of self contained, closed products has also been added.

Paragraph (a) provides that access features must be built-into a self contained, closed product rather than requiring users to attach an assistive device to the product. Personal headsets are not considered assistive technology and may be required to use the product. (See § 1194.23(f)(1) in the NPRM.)

*Comment.* Though discussed in the preamble, the text of the proposed rule did not address the issue of personal headsets. The preamble noted that personal headsets were not considered assistive technology. The ITIC urged the Board to make this clear in the text of the rule.

*Response.* The Board has modified this provision by clarifying that personal headsets are not considered assistive technology. No other changes were made to this provision.

Paragraph (b) addresses access problems that can arise when self contained, closed products require a response from a user within a certain time and is identical to § 1194.22(p) and § 1194.23(d) which are discussed in detail above. (See § 1194.21(d) in the NPRM.) The final rule requires only that a user be notified if a process is about to time-out and be given an opportunity to answer a prompt asking whether additional time is needed.

Paragraph (c) requires that when a product utilizes touchscreens or contact-sensitive controls, a method of operating the product be provided that complies with the provisions for controls in § 1194.23(k)(1) through (4). (See § 1194.21(f) in the NPRM.)

*Comment.* The proposed rule required that touchscreens or touch-operated controls be operable without requiring body contact or close human body proximity. Commenters found the proposed provision to be confusing. One commenter noted that the proposed rule required all touchscreens to be operable by a remote control. Several commenters expressed concern that accessibility to touchscreens for individuals who are blind or who have low vision was not adequately addressed.

*Response.* Touchscreens and other controls that operate by sensing a person's touch pose access problems for a range of persons with disabilities. This provision does not prohibit the use of touchscreens and contact sensitive controls, but, as modified, the final rule requires a redundant set of controls that can be used by persons who have access problems with touchscreens.

Paragraph (d) addresses the use of biometric controls. Biometric controls refer to controls that are activated only if particular biological features (*e.g.,* fingerprint, retina pattern, etc.) of the user matches specific criteria. Using retinal scans or fingerprint identification may become a common practice as a method of allowing an individual to gain access to personal data from an information transaction type of machine. (See § 1194.21(e) in the NPRM.)

*Comment.* In the proposed rule, the Board sought comment on the best approach to accessibility issues raised by biometric forms of identification and controls. Commenters responded that asking a system to have multiple forms of biometric identification could be prohibitively expensive. Most commenters were in agreement that biometric controls provide the most security. However, they also agreed that when such a system needs to be accessed by a person with a disability and that disability prohibits the use of a specific biometric feature, a non-biometric alternative should be provided that does not compromise security.

*Response.* The provision does not require a specific alternative. That selection is left up to the agency, which may choose a less expensive form of identification. No changes were made to this provision in the final rule.

Paragraph (e) requires that when products use audio as a way to communicate information, the auditory signal will be available through an industry standard connector at a standard signal level. Individuals using personal headphones, amplifiers, audio couplers, and other audio processing devices need a place to plug these devices into the product in a standard fashion. This gives the user the ability to listen privately to the information. The product must also provide a method to pause, restart, and interrupt the flow of information. (See § 1194.23(f)(2) and § 1194.25(d) in the NPRM.) No substantive comments were received on this provision and no changes were made, other than editorial changes.

Paragraph (f) provides that when products deliver voice output, they shall provide incremental volume control with output amplification up to a level of at least 65 dB. Where the ambient noise level of the environment is above 45 dB, a volume gain of at least 20 dB above the ambient level shall be user selectable. According to the Occupational Safety and Health Administration, and the American Speech, Language, and Hearing Association, 65 dB is the volume level for normal speech. This provision requires that audio output from a kiosk type product shall have a minimum level of 65 dB. For people with reduced hearing, voice levels must be 20 dB above the surround sound level to be understandable. This means that as long as the noise level in the surrounding environment is below 45 dB, the 65 dB output level would be sufficient. If the product is in an environment with a high noise level, the user must be able to raise the volume to a setting of 20 dB higher than the ambient level. (See § 1194.23(f)(3) in the NPRM.) A feature has been required to automatically reset the volume to the default level after every use. This is consistent with a similar provision addressing telecommunications products. No substantive comments were received and no other changes have been made to this section in the final rule.

Paragraph (g) addresses the use of color prompting and is identical to section 1194.21(i) discussed above. (See § 1194.21(a) in the NPRM.) No substantive comments were received and no changes have been made to this section in the final rule.

Paragraph (h) addresses color selection and contrast settings and is identical to section 1194.21(j) discussed above. (See § 1194.23(b)(8) in the NPRM.)

Paragraph (i) addresses the use of flashing objects and is identical to section 1194.21(k) discussed above. (See § 1194.21(c) in the NPRM.)

Paragraphs (j)(1) through (4) provide provisions for the physical characteristics of large office equipment including reach ranges and the general physical accessibility of controls and features. Examples of these products, include but are not limited to, copiers, information kiosks and floor standing printers. These provisions are based on the Americans with Disabilities Act Accessibility Guidelines (ADAAG 4.2 Space Allowance and Reach Ranges). Two figures are provided to help explain the application of these provisions. (See § 1194.21(b)(1) through (4) in the NPRM.) No substantive comments were received on these provisions and no changes were made in the final rule.

### *Section 1194.26 Desktop and Portable Computers*

This section is a result of the reorganization of the final rule. Paragraphs (a) through (d) contain provisions that apply to desktop and portable computers. The provisions in § 1194.21 for software address the accessibility of programs and operating systems that run on a computer. In contrast, the provisions in this section address physical characteristics of computer systems including the design of controls and the use of connectors. This section was previously addressed in § 1194.21 (General requirements), § 1194.23 (Component specific requirements) and § 1194.25 (Requirements for compatibility with assistive technology) in the NPRM.

Paragraph (a) addresses keyboards and other mechanically operated controls. These provisions are addressed further in sections 1194.23(k)(1) through (4) above. (See § 1194.23(a) in the NPRM.)

Paragraph (b) provides that systems using touchscreen technology must also provide controls that comply with sections 1194.23(k)(1) through (4) discussed above. (See § 1194.21(f) in the NPRM.) Similar to § 1194.25(c), this provision was modified in the final rule to require redundant controls.

Paragraph (c) requires that when biometric forms of identification are used, an alternative must also be available. This provision is identical to § 1194.25 (d) discussed above.

Paragraph (d) requires that products have standard ports and connectors. This means that the connection points on a system must comply with a standard specification that is available to other manufacturers. This provision assures that the designers of assistive technology will have access to information concerning the design of system connections and thus be able to produce products that can utilize those connections. (See § 1194.25(b) in the NPRM.)

*Comment.* In the proposed rule, this provision was addressed in § 1194.25(b) under the requirements for compatibility with assistive technology. A commenter noted that this provision was more specific to computer products and not to all products.

*Response.* As noted, this provision has been modified to apply to computer products.

## Subpart C—Functional Performance Criteria

### *Section 1194.31 Functional Performance Criteria*

This section provides functional performance criteria for overall product evaluation and for technologies or components for which there is no specific requirement under other sections. These criteria are also intended to ensure that the individual accessible components work together to create an accessible product. This section requires that all product functions, including operation and information retrieval, be operable through at least one mode addressed in each of the following paragraphs.

*Comment.* The ITIC requested clarification as to how a manufacturer would determine the type and number of assistive technology devices for which support must be provided by a product.

*Response.* Manufacturers do not need to be aware of the universe of assistive technology products on the market. Each provision specifies the type of assistive technology that must be supported. For example, § 1194.31(a) addresses those assistive technology devices which provide output to persons who cannot see the screen. Such devices may include screen readers, Braille displays and speech synthesizers. There are numerous resources available to manufacturers to assist them in identifying specific types of assistive technology which would be used to access their product.

Paragraph (a) provides that at least one mode of operation and information retrieval that does not require user vision shall be provided, or support for assistive technology used by people who are blind or visually impaired shall be provided. It is not expected that every software program will be self-voicing or have its own built-in screen reader. Software that complies with § 1194.21 would also satisfy this provision. (See § 1194.27(a) in the NPRM.) No substantive comments were received regarding this provision and no changes were made in the final rule.

Paragraph (b) provides that at least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 (when corrected with glasses) must be provided in audio and enlarged print output that works together or independently. In the alternative, support for assistive technology used by people who are blind or who have low vision must be provided. Although visual acuity of 20/200 is considered ''legally blind,'' there are actually millions of Americans with vision below the 20/200 threshold who can still see enough to operate and get output from technology, often with just a little additional boost in contrast or font size. This paragraph requires either the provision of screen enlargement and voice output or, that the product support assistive technology. (See § 1194.27(b) in the NPRM.) No substantive comments were received regarding this provision and no changes were made in the final rule.

Paragraph (c) provides that at least one mode of operation and information retrieval that does not require user hearing must be provided, or support for assistive technology used by people who are deaf or hard of hearing shall be provided. This provision is met when a product provides visual redundancy for any audible cues or audio output. If this redundancy cannot be built-into a product then the product shall support the use of assistive technology. (See § 1194.27(c) in the NPRM.) No substantive comments were received regarding this provision and no changes were made in the final rule.

Paragraph (d) requires that audio information important for the use of a product, must be provided in an enhanced auditory fashion by allowing for an increase in volume and/or altering the tonal quality or increasing the signal-to-noise ratio. For example, increasing the output would assist persons with limited hearing to receive information. Audio information that is important for the use of a product includes, but is not limited to, error tones, confirmation beeps and tones, and verbal instructions. (See § 1194.27(d) in the NPRM.) No substantive comments were received regarding this provision. The final provision has been amended editorially to provide that support for assistive hearing devices may be provided in place of built-in enhanced audio features.

Paragraph (e) provides that at least one mode of operation and information retrieval which does not require user speech must be provided, or support for assistive technology shall be provided. Most products do not require speech input. However, if speech input is required to operate a product, this paragraph requires that at least one alternative input mode also be provided. For example, an interactive telephone menu that requires the user to say or press ''one'' would meet this provision. (See § 1194.27(e) in the NPRM.) No substantive comments were received regarding this provision and no changes were made in the final rule.

Paragraph (f) provides that at least one mode of operation and information retrieval that does not require fine motor control or simultaneous actions and which is operable with limited reach and strength must be provided. (See § 1194.27(f) in the NPRM.) No substantive comments were received regarding this provision and no changes were made in the final rule.

### Subpart D—Information, Documentation, and Support

*Section 1194.41 Information, Documentation, and Support*

In order for a product to be fully usable by persons with disabilities, the information about the product and product support services must also be usable by persons with disabilities. These issues are addressed in this section.

Paragraph (a) states that when an agency provides end-user documentation to users of technology, the agency must ensure that the documentation is available upon request in alternate formats. Alternate formats are defined in § 1194.4, Definitions. Except as provided in paragraph (b) below, this provision does not require alternate formats of documentation that is not provided by the agency to other users of technology. (See § 1194.31(a) in the NPRM.) No substantive comments were received regarding this provision and no changes other than editorial changes were made in the final rule.

Paragraph (b) requires that agencies supply end-users with information about accessibility or compatibility features that are built-into a product, upon request. (See § 1194.31(b) in the NPRM.) No substantive comments were received regarding this provision and, other than an editorial revision substituting ''methods'' for ''modes'', and general editorial changes, no other changes were made in the final rule.

Paragraph (c) provides that help desks and other support services serving an agency must be capable of accommodating the communications needs of persons with disabilities. For example, an agency help desk may need to communicate through a TTY. The help desk or support service must also be familiar with such features as keyboard access and other options important to people with disabilities. (See § 1194.31(a) in the NPRM.) No substantive comments were received regarding this provision and no changes other than editorial changes were made in the final rule.

### Regulatory Process Matters

*Executive Order 12866: Regulatory Planning and Review and Congressional Review Act*

This final rule is an economically significant regulatory action under Executive Order 12866 and has been reviewed by the Office of Management and Budget (OMB). The final rule is also a major rule under the Congressional Review Act. The Board has prepared a regulatory assessment for the final rule which has been placed in the docket and is available for public inspection. The regulatory assessment is also available on the Board's Internet site (http://www.access-board.gov/sec508/assessment.htm). In the NPRM, the Board sought comment on the regulatory assessment which was prepared in conjunction with the proposed rule. The Board received four comments that specifically addressed concerns with that economic assessment. A summary of the comments received and the Board's responses can be found in Chapter Six of the Board's final regulatory assessment.

Section 508 covers the development, procurement, maintenance or use of electronic and information technology by Federal agencies. Exemptions are provided by statute for national security systems and for instances where compliance would impose an undue burden on an agency. The final rule improves the accessibility of electronic and information technology used by the Federal government and will affect Federal employees with disabilities, as well as members of the public with disabilities who seek to use Federal electronic and information technologies to access information. The final rule is based largely on the recommendations of the Electronic and Information Technology Access Advisory Committee.

The standards in the final rule will be incorporated into the Federal Acquisition Regulation (FAR). Failure of a Federal agency to comply with the standards may result in a complaint under the agency's existing complaint procedures under section 504 of the

Rehabilitation Act or a civil action seeking to enforce compliance with the standards.

### Estimated Baseline of Federal Spending for Electronic and Information Technology

According to OMB figures, Federal government expenditures for information technology products was $37.6 billion in fiscal year 1999. The defense agencies appear to have the highest information technology budgets, while civilian agency budgets are expected to increase rapidly. It was not possible however, to disaggregate this data such that it was useful for purposes of a regulatory assessment. Instead, the regulatory assessment uses annual sales data collected from the General Services Administration (GSA) as a proxy for the actual number of products in each applicable technology category. Using the GSA data, the regulatory assessment estimates that the Federal government spends approximately $12.4 billion annually on electronic and information technology products covered by the final rule. This estimate likely understates the actual spending by the Federal government because it is limited to the GSA data. Agencies are not required to make purchases through the GSA supply service, thus many items are purchased directly from suppliers. As a result, the government costs for software and compatible hardware products may actually be higher than estimates would indicate.

The regulatory assessment also examines historical budgetary obligations for information technology tracked by OMB until fiscal year 1998. Two scenarios were examined to develop an upper and lower bound to represent the proportion expected to be potentially affected by the final rule. During a five year period from fiscal year 1994 through fiscal year 1998, the average proportion of the total information technology obligations potentially covered by the final rule ranged between 25 percent and 50 percent. The $12.4 billion GSA estimate falls within this range, representing 33 percent of the total fiscal year 1999 information technology obligations of $37.6 billion. One limitation of these ranges is that they are based on gross classifications of information technology obligations and do not provide the level of disaggregation necessary to parallel the GSA data assessment. As a result, the two scenarios likely include expenditures on products and services that would not be effected by the final rule to a higher degree than the data obtained from GSA.

The degree to which the potential understatement of baseline spending leads to an understatement of the cost of the final rule is unclear. Some of the components of the estimated cost of the final rule rely heavily on the level of Federal spending while others are independent of this number.

### Estimated Cost of the Final Rule

The regulatory assessment includes both direct and opportunity costs associated with the final rule. Major sources of cost include:

- Costs of modifying electronic and information technology to meet the substantive requirements of the standards;
- Training of staff, both Federal and manufacturers, to market, support, and use technologies modified in response to the standards; and
- Translation of documentation and instructions into alternate formats.

The direct costs that were quantified are shown in Table 1. The total quantified costs to society range from $177 million to $1,068 million annually. The Federal proportion of these costs is estimated to range between $85 million and $691 million. The ability of manufacturers, especially software manufacturers, to distribute these costs over the general consumer population will determine the actual proportion shared by the Federal government. Assuming that the addition of accessibility features add value to the products outside the Federal government, it is expected that the costs will be distributed across society thereby setting a lower bound cost to the Federal government of $85 million. If manufacturers do not distribute the costs across society, the upper bound of the Federal cost will increase to an estimated $1,068 million. These costs must be placed in appropriate context by comparing them with the total Federal expenditures for information technology. By comparison, the lower and upper bound of the incremental costs represent a range of 0.23 percent to 2.8 percent of the $37.6 billion spent by the Federal government on information technology in fiscal year 1999. Although the regulatory assessment does not analyze the timing of expenditures or reductions in costs over time, it is expected that the costs will decrease over time as a proportion of total electronic and information technology spending.

TABLE 1

| Electronic and information technology | Lower bound cost estimates (millions) | Upper bound cost estimates (millions) |
|---|---|---|
| General Office Software | $110 | $456 |
| Mission Specific Software | 10 | 52 |
| Compatible Hardware Products | .................... | 337 |
| Document Management Products | 56 | 222 |
| Microphotographic Products | 0.1 | 0.4 |
| Other Miscellaneous Products | 0.2 | 1 |
| Total Social Cost | 177 | 1,068 |
| Estimated Federal Proportion | 85 | [1] 691 |

[1] As noted above, if manufacturers do not distribute the costs across society, the upper bound of the Federal cost will increase to an estimated $1,068 million.

Accessible alternatives are available to satisfy the requirements of the final rule for many types of electronic and information technologies, particularly computers and software products. Some electronic and information technology products will require modifications to meet the requirements of the final standards.

For many types of electronic and information technology, the final rule focuses on compatibility with existing and future assistive devices, such as screen readers. The final rule does not require that assistive technologies be provided universally. Provision of assistive technologies is still governed by the reasonable accommodation requirements contained in sections 501 and 504 of the Rehabilitation Act. Section 508 does not require that assistive devices be purchased, but it does require that covered electronic and information technology be capable of having such devices added at some later time as necessary.

Software products represent the largest part of the estimated costs. The regulatory assessment assumes that Federal software expenditures can be divided into two major subcategories: general office applications and mission-specific applications. Internet applications are assumed to be represented within each of these subcategories. General office applications include operating systems, wordprocessors, and spreadsheets, and are assumed to represent 80 percent of the total software category. The remaining 20 percent covers mission-specific or proprietary applications that have limited distribution outside the Federal government. Within each subcategory, the estimated costs of the final rule are distributed according to the level or degree of accessibility already being achieved in the private sector.

The general office application subcategory is broken into three groups based on discussions with several industry experts. The first 30 percent is expected to require very little modification to satisfy the final standards and therefore no incremental cost is associated with this group. The middle 40 percent is expected to require minor to medium alterations to satisfy the final rule. The cost of modifying a particular general office application in this category is estimated to be in the range of 0.4 percent to 1 percent based on discussions with several manufacturers. This assumption is based on the ratio of employees dedicated to accessibility issues. The methodology uses employee classification as a proxy for cost or expense of accessibility research and development, labor, and design that are all factored into the final product cost. The remaining 30 percent is expected to require significant modifications to meet the requirements of the final rule, which is estimated to cost in the range of 1 percent to 5 percent based on discussion with industry experts.

The regulatory assessment assumes that the remaining 20 percent of the software products purchased by the Federal government represent proprietary or mission-specific software with limited distribution outside the government. These products will require significant modification to satisfy the final rule. Based on discussions with industry experts, the cost increase associated with achieving the level of accessibility required by the final rule is estimated to range from 1 percent to 5 percent.

Estimated Benefits of the Final Rule

The benefits associated with the final rule results from increased access to electronic and information technology for Federal employees with disabilities and members of the public seeking Federal information provided using electronic and information technology. This increased access reduces barriers to employment in the Federal government for persons with disabilities, reduces the probability that Federal employees with disabilities will be underemployed, and increases the productivity of Federal work teams. The final standards may also have benefits for people outside the Federal workforce, both with and without disabilities, as a result of spillover of technology from the Federal government to the rest of society.

Two methods are presented in the regulatory assessment for evaluating the quantifiable benefits of the final rule. The first is a wage gap analysis that attempts to measure the difference in wages between the general Federal workforce and Federal workers with targeted and reportable disabilities. While this analysis is limited to white collar Federal workers due to data constraints, the potential change in productivity is measured by the difference between the weighted average salary for all white collar Federal employees and the average within the two disability classes. This assumes that an increase in accessibility will help diminish this wage gap by increasing worker productivity.

The alternative is a team based approach for measuring the productivity of Federal workers. This approach is based on the assumption that a Federal workers wage rate reflects their productivity and the scarcity of their skills in the labor market. However this may not apply to Federal wage rates, thus the average productivity of a Federal team is assumed to be equivalent to the average Federal wage rate. Based on this average rate, it is assumed that the final rule will produce an increase in productivity ranging between 5 percent and 10 percent.

Since no data have been identified to support the increase in productivity in the team based approach, the wage gap analysis is used to represent the benefits generated by the final rule shown in Table 2. Keeping in mind certain data limitations with this analysis, the benefits derived from the wage gap method do not account for benefits that may be accrued by the general public or other Federal workers due to spillover effects of increased accessibility resulting from the final standards.

TABLE 2

| Productivity increase | Aggregate benefits range (millions) |
|---|---|
| Lower Bound | |
| Upper Bound | $466 |

Not all government policies are based on maximizing economic efficiency. Some policies are based on furthering the rights of certain classes of individuals to achieve more equitable results, regardless of the effect on economic efficiency. Accessibility to electronic information and technology is an essential component of civil rights for persons with disabilities. The final rule will ensure that Federal employees with disabilities will have access to electronic and information technology used by the Federal government that is comparable to that of Federal employees without disabilities; and that members of the public with disabilities will have comparable access to information and services provided to members of the public without disabilities through the use of Federal electronic and information technology.

Based on Bureau of Census statistics from 1994, 20.6 percent or 54 million persons in the United States have some level of disability. By increasing the accessibility of electronic and information technology used by the Federal government, the final rule may also improve future employment opportunities in the Federal government for persons with disabilities currently employed by the Federal government, and for persons that are working in the private sector or are classified as not being active in the labor force. Increasing the accessibility of electronic and information technology increases the productivity and mobility of the disabled sector of the labor pool that, under existing conditions, may face barriers to their employment and advancement within the Federal workforce and in the private sector. The standards will allow other Federal workers who become temporarily disabled to maintain their productivity during their illness. In addition, accessible features of electronic and information technology may also enhance the productivity of Federal workers without disabilities and therefore be a benefit to the workforce in general.

*Regulatory Flexibility Act*

The Regulatory Flexibility Act (RFA) (5 U.S.C. 601 *et seq.*), as amended, generally requires Federal agencies to conduct a regulatory flexibility analysis describing the impact of the regulatory action on small entities. However, section 605(b) of the RFA, provides that a regulatory flexibility analysis is not required if the rule will not have a significant economic impact on a substantial number of small entities. This final rule imposes requirements only on the Federal Government and the Board certifies that it does not impose any requirements on small entities. As a result, a regulatory flexibility analysis is not required.

*Executive Order 13132: Federalism*

By its terms, this rule applies to the development, procurement, maintenance or use by Federal agencies of electronic and information technology. As such, the Board believes that it does not have federalism implications within the meaning of Executive Order 13132. In the proposed rule, the Board referred to the Department of Education's interpretation of the Assistive Technology Act (the ''AT Act''), 29 U.S.C. 3001. The Board received approximately five responses from various State organizations regarding the relationship between the AT Act and Section 508 of the Rehabilitation Act. The Department of Education, the agency responsible for administering the AT Act, has advised the Board that it plans to work with States to address the relationship between the AT Act and section 508, and specifically how the Board's standards would apply to the States for purposes of the AT Act. As part of this process, the Department of Education will address issues raised in the five responses the Board received on the relationship between the AT Act and section 508 of the Rehabilitation Act.

*Unfunded Mandates Reform Act*

The Unfunded Mandates Reform Act does not apply to proposed or final rules that enforce constitutional rights of individuals or enforce any statutory rights that prohibit discrimination on the basis of race, color, sex, national origin, age, handicap, or disability. Since the final rule is issued under the authority of section 508, part of title V of the Rehabilitation Act of 1973 which establishes civil rights protections for individuals with disabilities, an assessment of the rule's effects on State, local, and tribal governments, and the private sector is not required by the Unfunded Mandates Reform Act.

**List of Subjects in 36 CFR Part 1194**

Civil rights, Communications equipment, Computer technology, Electronic products, Government employees, Government procurement, Individuals with disabilities, Reporting and recordkeeping requirements, Telecommunications.

**Thurman M. Davis, Sr.,**
*Chair, Architectural and Transportation Barriers Compliance Board.*

For the reasons set forth in the preamble, the Board adds part 1194 to Chapter XI of title 36 of the Code of Federal Regulations to read as follows:

## PART 1194—ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY STANDARDS

**Subpart A—General**

**Subpart B—Technical Standards**

**Subpart C—Functional Performance Criteria**

**Subpart D—Information, Documentation, and Support**

**Figures to Part 1194**

**Authority:** 29 U.S.C. 794d.

### Subpart A—General

**§ 1194.1 Purpose.**

The purpose of this part is to implement section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d). Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

**§ 1194.2 Application.**

(a) Products covered by this part shall comply with all applicable provisions of this part. When developing, procuring, maintaining, or using electronic and information technology, each agency shall ensure that the products comply with the applicable provisions of this part, unless an undue burden would be imposed on the agency.

(1) When compliance with the provisions of this part imposes an undue burden, agencies shall provide individuals with disabilities with the information and data involved by an alternative means of access that allows the individual to use the information and data.

(2) When procuring a product, if an agency determines that compliance with any provision of this part imposes an undue burden, the documentation by the agency supporting the procurement shall explain why, and to what extent, compliance with each such provision creates an undue burden.

(b) When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards.

(c) Except as provided by § 1194.3(b), this part applies to electronic and information technology developed, procured, maintained, or used by agencies directly or used by a contractor under a contract with an agency which requires the use of such product, or requires the use, to a significant extent, of such product in the performance of a service or the furnishing of a product.

**§ 1194.3 General exceptions.**

(a) This part does not apply to any electronic and information technology operated by agencies, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or systems which are critical to the direct fulfillment of military or intelligence missions. Systems which are critical to the direct fulfillment of military or intelligence missions do not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(b) This part does not apply to electronic and information technology that is acquired by a contractor incidental to a contract.

(c) Except as required to comply with the provisions in this part, this part does not require the installation of specific accessibility-related software or the attachment of an assistive technology device at a workstation of a Federal employee who is not an individual with a disability.

(d) When agencies provide access to the public to information or data through electronic and information technology, agencies are not required to make products owned by the agency available for access and use by individuals with disabilities at a location other than that where the electronic and information technology is provided to the public, or to purchase products for access and use by individuals with disabilities at a location other than that where the electronic and information technology is provided to the public.

(e) This part shall not be construed to require a fundamental alteration in the nature of a product or its components.

(f) Products located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment are not required to comply with this part.

### § 1194.4 Definitions.

The following definitions apply to this part:

*Agency.* Any Federal department or agency, including the United States Postal Service.

*Alternate formats.* Alternate formats usable by people with disabilities may include, but are not limited to, Braille, ASCII text, large print, recorded audio, and electronic formats that comply with this part.

*Alternate methods.* Different means of providing information, including product documentation, to people with disabilities. Alternate methods may include, but are not limited to, voice, fax, relay service, TTY, Internet posting, captioning, text-to-speech synthesis, and audio description.

*Assistive technology.* Any item, piece of equipment, or system, whether acquired commercially, modified, or customized, that is commonly used to increase, maintain, or improve functional capabilities of individuals with disabilities.

*Electronic and information technology.* Includes information technology and any equipment or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information. The term electronic and information technology includes, but is not limited to, telecommunications products (such as telephones), information kiosks and transaction machines, World Wide Web sites, multimedia, and office equipment such as copiers and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

*Information technology.* Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

*Operable controls.* A component of a product that requires physical contact for normal operation. Operable controls include, but are not limited to, mechanically operated controls, input and output trays, card slots, keyboards, or keypads.

*Product.* Electronic and information technology.

*Self Contained, Closed Products.* Products that generally have embedded software and are commonly designed in such a fashion that a user cannot easily attach or install assistive technology. These products include, but are not limited to, information kiosks and information transaction machines, copiers, printers, calculators, fax machines, and other similar types of products.

*Telecommunications.* The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

*TTY.* An abbreviation for teletypewriter. Machinery or equipment that employs interactive text based communications through the transmission of coded signals across the telephone network. TTYs may include, for example, devices known as TDDs (telecommunication display devices or telecommunication devices for deaf persons) or computers with special modems. TTYs are also called text telephones.

*Undue burden.* Undue burden means significant difficulty or expense. In determining whether an action would result in an undue burden, an agency shall consider all agency resources available to the program or component for which the product is being developed, procured, maintained, or used.

### § 1194.5 Equivalent facilitation.

Nothing in this part is intended to prevent the use of designs or technologies as alternatives to those prescribed in this part provided they result in substantially equivalent or greater access to and use of a product for people with disabilities.

## Subpart B—Technical Standards

### § 1194.21 Software applications and operating systems.

(a) When software is designed to run on a system that has a keyboard, product functions shall be executable from a keyboard where the function itself or the result of performing a function can be discerned textually.

(b) Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer.

(c) A well-defined on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that assistive technology can track focus and focus changes.

(d) Sufficient information about a user interface element including the identity, operation and state of the element shall be available to assistive technology. When an image represents a program element, the information conveyed by the image must also be available in text.

(e) When bitmap images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance.

(f) Textual information shall be provided through operating system functions for displaying text. The minimum information that shall be made available is text content, text input caret location, and text attributes.

(g) Applications shall not override user selected contrast and color selections and other individual display attributes.

(h) When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user.

(i) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

(j) When a product permits a user to adjust color and contrast settings, a variety of color selections capable of producing a range of contrast levels shall be provided.

(k) Software shall not use flashing or blinking text, objects, or other elements having a flash or blink frequency greater than 2 Hz and lower than 55 Hz.

(l) When electronic forms are used, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.

### § 1194.22 Web-based intranet and internet information and applications.

(a) A text equivalent for every non-text element shall be provided (*e.g.,* via ''alt'', ''longdesc'', or in element content).

(b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.

(c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.

(d) Documents shall be organized so they are readable without requiring an associated style sheet.

(e) Redundant text links shall be provided for each active region of a server-side image map.

(f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.

(g) Row and column headers shall be identified for data tables.

(h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.

(i) Frames shall be titled with text that facilitates frame identification and navigation.

(j) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.

(k) A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.

(l) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by assistive technology.

(m) When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with § 1194.21(a) through (l).

(n) When electronic forms are designed to be completed on-line, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.

(o) A method shall be provided that permits users to skip repetitive navigation links.

(p) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.

**Note to § 1194.22:** 1. The Board interprets paragraphs (a) through (k) of this section as consistent with the following priority 1 Checkpoints of the Web Content Accessibility Guidelines 1.0 (WCAG 1.0) (May 5, 1999) published by the Web Accessibility Initiative of the World Wide Web Consortium:

| Section 1194.22 paragraph | WCAG 1.0 checkpoint |
|---|---|
| (a) | 1.1 |
| (b) | 1.4 |
| (c) | 2.1 |
| (d) | 6.1 |
| (e) | 1.2 |
| (f) | 9.1 |
| (g) | 5.1 |
| (h) | 5.2 |
| (i) | 12.1 |
| (j) | 7.1 |
| (k) | 11.4 |

2. Paragraphs (l), (m), (n), (o), and (p) of this section are different from WCAG 1.0. Web pages that conform to WCAG 1.0, level A (*i.e.,* all priority 1 checkpoints) must also meet paragraphs (l), (m), (n), (o), and (p) of this section to comply with this section. WCAG 1.0 is available at http://www.w3.org/TR/1999/WAI–WEBCONTENT–19990505.

### § 1194.23 Telecommunications products.

(a) Telecommunications products or systems which provide a function allowing voice communication and which do not themselves provide a TTY functionality shall provide a standard non-acoustic connection point for TTYs. Microphones shall be capable of being turned on and off to allow the user to intermix speech with TTY use.

(b) Telecommunications products which include voice communication functionality shall support all commonly used cross-manufacturer non-proprietary standard TTY signal protocols.

(c) Voice mail, auto-attendant, and interactive voice response telecommunications systems shall be usable by TTY users with their TTYs.

(d) Voice mail, messaging, auto-attendant, and interactive voice response telecommunications systems that require a response from a user within a time interval, shall give an alert when the time interval is about to run out, and shall provide sufficient time for the user to indicate more time is required.

(e) Where provided, caller identification and similar telecommunications functions shall also be available for users of TTYs, and for users who cannot see displays.

(f) For transmitted voice signals, telecommunications products shall provide a gain adjustable up to a minimum of 20 dB. For incremental volume control, at least one intermediate step of 12 dB of gain shall be provided.

(g) If the telecommunications product allows a user to adjust the receive volume, a function shall be provided to automatically reset the volume to the default level after every use.

(h) Where a telecommunications product delivers output by an audio transducer which is normally held up to the ear, a means for effective magnetic wireless coupling to hearing technologies shall be provided.

(i) Interference to hearing technologies (including hearing aids, cochlear implants, and assistive listening devices) shall be reduced to the lowest possible level that allows a user of hearing technologies to utilize the telecommunications product.

(j) Products that transmit or conduct information or communication, shall pass through cross-manufacturer, non-proprietary, industry-standard codes, translation protocols, formats or other information necessary to provide the information or communication in a usable format. Technologies which use encoding, signal compression, format transformation, or similar techniques shall not remove information needed for access or shall restore it upon delivery.

(k) Products which have mechanically operated controls or keys, shall comply with the following:

(1) Controls and keys shall be tactilely discernible without activating the controls or keys.

(2) Controls and keys shall be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys shall be 5 lbs. (22.2 N) maximum.

(3) If key repeat is supported, the delay before repeat shall be adjustable to at least 2 seconds. Key repeat rate shall be adjustable to 2 seconds per character.

(4) The status of all locking or toggle controls or keys shall be visually discernible, and discernible either through touch or sound.

### § 1194.24 Video and multimedia products.

(a) All analog television displays 13 inches and larger, and computer equipment that includes analog television receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals. As soon as practicable, but not later than July 1, 2002, widescreen digital television (DTV) displays measuring at least 7.8 inches vertically, DTV sets with conventional displays measuring at least 13 inches vertically, and stand-alone DTV tuners, whether or not they are marketed with display screens, and computer equipment that includes DTV receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals.

(b) Television tuners, including tuner cards for use in computers, shall be equipped with secondary audio program playback circuitry.

(c) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain speech or other audio information necessary for the comprehension of the content, shall be open or closed captioned.

(d) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain visual information necessary for the comprehension of the content, shall be audio described.

(e) Display or presentation of alternate text presentation or audio descriptions shall be user-selectable unless permanent.

### § 1194.25 Self contained, closed products.

(a) Self contained products shall be usable by people with disabilities without requiring an end-user to attach assistive technology to the product. Personal headsets for private listening are not assistive technology.

(b) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.

(c) Where a product utilizes touchscreens or contact-sensitive controls, an input method shall be provided that complies with § 1194.23 (k) (1) through (4).

(d) When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.

(e) When products provide auditory output, the audio signal shall be provided at a standard signal level through an industry standard connector that will allow for private listening. The product must provide the ability to interrupt, pause, and restart the audio at anytime.

(f) When products deliver voice output in a public area, incremental volume control shall be provided with output amplification up to a level of at least 65 dB. Where the ambient noise level of the environment is above 45 dB, a volume gain of at least 20 dB above the ambient level shall be user selectable. A function shall be provided to automatically reset the volume to the default level after every use.

(g) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

(h) When a product permits a user to adjust color and contrast settings, a range of color selections capable of producing a variety of contrast levels shall be provided.

(i) Products shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.

(j) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following:

(1) The position of any operable control shall be determined with respect to a vertical plane, which is 48 inches in length, centered on the operable control, and at the maximum protrusion of the product within the 48 inch length (see Figure 1 of this part).

(2) Where any operable control is 10 inches or less behind the reference plane, the height shall be 54 inches maximum and 15 inches minimum above the floor.

(3) Where any operable control is more than 10 inches and not more than 24 inches behind the reference plane, the height shall be 46 inches maximum and 15 inches minimum above the floor.

(4) Operable controls shall not be more than 24 inches behind the reference plane (see Figure 2 of this part).

### § 1194.26 Desktop and portable computers.

(a) All mechanically operated controls and keys shall comply with § 1194.23(k)(1) through (4).

(b) If a product utilizes touchscreens or touch-operated controls, an input method shall be provided that complies with § 1194.23 (k) (1) through (4).

(c) When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.

(d) Where provided, at least one of each type of expansion slots, ports and connectors shall comply with publicly available industry standards.

## Subpart C—Functional Performance Criteria

### § 1194.31 Functional performance criteria.

(a) At least one mode of operation and information retrieval that does not require user vision shall be provided, or support for assistive technology used by people who are blind or visually impaired shall be provided.

(b) At least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 shall be provided in audio and enlarged print output working together or independently, or support for assistive technology used by people who are visually impaired shall be provided.

(c) At least one mode of operation and information retrieval that does not require user hearing shall be provided, or support for assistive technology used by people who are deaf or hard of hearing shall be provided.

(d) Where audio information is important for the use of a product, at least one mode of operation and information retrieval shall be provided in an enhanced auditory fashion, or support for assistive hearing devices shall be provided.

(e) At least one mode of operation and information retrieval that does not require user speech shall be provided, or support for assistive technology used by people with disabilities shall be provided.

(f) At least one mode of operation and information retrieval that does not require fine motor control or simultaneous actions and that is operable with limited reach and strength shall be provided.

## Subpart D—Information, Documentation, and Support

### § 1194.41 Information, documentation, and support.

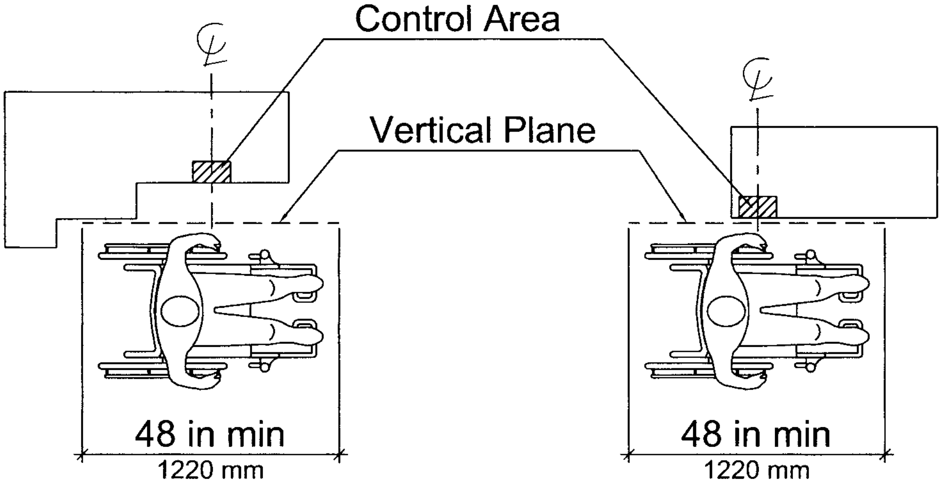
(a) Product support documentation provided to end-users shall be made available in alternate formats upon request, at no additional charge.

(b) End-users shall have access to a description of the accessibility and compatibility features of products in alternate formats or alternate methods upon request, at no additional charge.

(c) Support services for products shall accommodate the communication needs of end-users with disabilities.

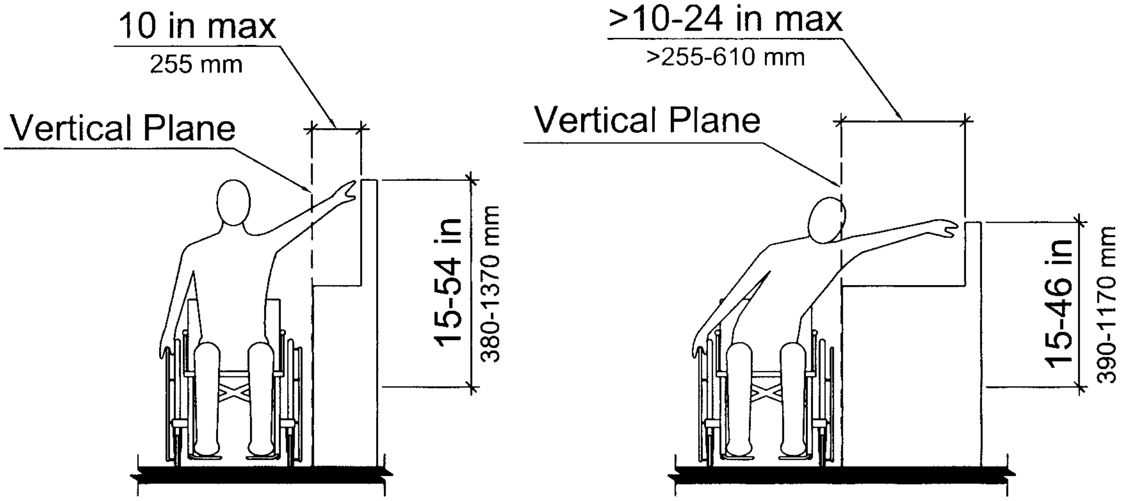
**Figures to Part 1194**

BILLING CODE 8150–01–P



Vertical Plane Relative to the Operable Control

Figure 1



Height of Operable Control Relative to the Vertical Plane

Figure 2

[FR Doc. 00–32017 Filed 12–20–00; 8:45 am]

**BILLING CODE 8150–01–P**

Federal Register

Friday,
March 31, 2000

## Part II

# Architectural and Transportation Barriers Compliance Board

36 CFR Part 1194

**Electronic and Information Technology Accessibility Standards; Proposed Rule**

**ARCHITECTURAL AND TRANSPORTATION BARRIERS COMPLIANCE BOARD**

**36 CFR Part 1194**

**[Docket No. 2000–01]**

**RIN 3014–AA25**

## Electronic and Information Technology Accessibility Standards

**AGENCY:** Architectural and Transportation Barriers Compliance Board.

**ACTION:** Notice of proposed rulemaking.

**SUMMARY:** The Architectural and Transportation Barriers Compliance Board (Access Board) proposes accessibility standards for electronic and information technology covered by section 508 of the Rehabilitation Act Amendments of 1998. Section 508 requires the Access Board to publish standards setting forth a definition of electronic and information technology and the technical and functional performance criteria necessary for accessibility for such technology. Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they shall ensure that the electronic and information technology allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

**DATES:** Comments should be received by May 30, 2000; however, late comments will be considered to the extent practicable.

**ADDRESSES:** Comments should be sent to the Office of Technical and Information Services, Architectural and Transportation Barriers Compliance Board, 1331 F Street NW., suite 1000, Washington, DC 20004–1111. Comments sent by e-mail will be considered only if they include the full name and address of the sender in the text. E-mail comments should be sent to section508nprm@access-board.gov. Comments will be available for inspection at the above address from 9:00 a.m. to 5:00 p.m. on regular business days.

**FOR FURTHER INFORMATION CONTACT:** Doug Wakefield, Office of Technical and Information Services, Architectural and Transportation Barriers Compliance Board, 1331 F Street, NW., suite 1000, Washington, DC 20004–1111. Telephone number (202) 272–5434 extension 139 (voice); (202) 272–5449 (TTY). Electronic mail address: wakefield@access-board.gov.

**SUPPLEMENTARY INFORMATION:**

### Availability of Copies and Electronic Access

Single copies of this publication may be obtained at no cost by calling the Access Board's automated publications order line (202) 272–5434, by pressing 2 on the telephone keypad, then 1, and requesting publication S–38 (Electronic and Information Technology Accessibility Standards Notice of Proposed Rulemaking). Persons using a TTY should call (202) 272–5449. Please record a name, address, telephone number and request publication S–38. This document is available in alternate formats upon request. Persons who want a copy in an alternate format should specify the type of format (cassette tape, Braille, large print, or ASCII disk). This document is also available on the Board's Internet site (http://www.access-board.gov/rules/508nprm.htm).

This proposed rule is based on recommendations of the Board's Electronic and Information Technology Access Advisory Committee. The report is available on the Board's Internet site (http://www.access-board.gov/pubs/eitaacrpt.htm).

### Background

On August 7, 1998, the President signed into law the Workforce Investment Act of 1998, which includes the Rehabilitation Act Amendments of 1998. Section 508 of the Rehabilitation Act Amendments requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they shall ensure that the electronic and information technology allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency.[1] Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities.

Section 508 was originally added to the Rehabilitation Act in 1986. It required the Secretary of Education and the Administrator of the General Services Administration to develop and establish guidelines for Federal agencies for electronic and information technology accessibility and required that such guidelines be revised, as necessary, to reflect technological advances or changes.[2] Section 508 also required each Federal agency to comply with the guidelines. However, there was no enforcement mechanism to provide for compliance. The changes to section 508 contained in the Rehabilitation Act Amendments of 1998 were designed to strengthen the previous law.

### Access Board Responsibilities

Section 508(a)(2)(A) of the Rehabilitation Act Amendments of 1998 requires the Architectural and Transportation Barriers Compliance Board (Access Board)[3] to publish standards setting forth a definition of electronic and information technology and the technical and functional performance criteria necessary for accessibility for such technology. If an agency determines that meeting these standards, when procuring electronic and information technology, imposes an undue burden, it must explain why meeting these standards creates an undue burden.

The definition of electronic and information technology is required to be

[1] Section 508 does not apply to national security systems, as that term is defined in section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).

[2] In October 1987, the Department of Education and the General Services Administration (GSA) issued section 508 guidelines which addressed management responsibilities and functional performance specifications for input, output, and documentation access to electronic equipment. On January 1, 1991, after receiving further comment from agencies, vendors, and individuals with disabilities, the GSA issued Bulletin C–8 containing these guidelines as amended, in the Federal Information Resources Management Regulations (FIRMR). In 1996 the FIRMR was eliminated.

[3] The Access Board is an independent Federal agency established by section 502 of the Rehabilitation Act (29 U.S.C. 792) whose primary mission is to promote accessibility for individuals with disabilities. The Access Board consists of 25 members. Thirteen are appointed by the President from among the public, a majority of who are required to be individuals with disabilities. The other twelve are heads of the following Federal agencies or their designees whose positions are Executive Level IV or above: The departments of Health and Human Services, Education, Transportation, Housing and Urban Development, Labor, Interior, Defense, Justice, Veterans Affairs, and Commerce; the General Services Administration; and the United States Postal Service.

consistent with the definition of information technology in section 5002(3) of the Clinger-Cohen Act of 1996.[4] (40 U.S.C. 1401(3)). Information technology under that law means ''any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information'' by a Federal agency.

In developing its standards, the Access Board is required to consult with various Federal agencies,[5] the electronic and information technology industry, and appropriate public or nonprofit agencies or organizations, including organizations representing individuals with disabilities. The Access Board is also required to periodically review and, as appropriate, amend the standards to reflect technological advances or changes in electronic and information technology. The General Services Administration and the Access Board are required to provide technical assistance to individuals and Federal agencies concerning the requirements of section 508.

## Other Section 508 Requirements

The Access Board was required to publish standards by February 7, 2000. For several reasons, the Board has not met that statutory deadline. Because the Board was required to consult with various affected interests, it created a Federal advisory committee. The advisory committee met from October 1998 through May 1999. Since then, the Board has met through an ad hoc group consisting of several Board members and Federal agency representatives to review the committee's recommendations and develop the proposed rule. Additionally, the Board contracted to prepare the regulatory assessment for the proposed rule. After the Board submitted the proposed rule to the Office of Management and Budget (OMB) for review under Executive Order 12866, OMB distributed the proposed rule twice to the Chief Information Officers for review and comment. The Board has also been coordinating its efforts with the Federal Acquisition Regulatory Council. Section 508(a)(3) provides that within six months after the Board publishes its standards, the Federal Acquisition Regulatory Council is required to revise the Federal Acquisition Regulation, and each Federal agency is required to revise the Federal procurement policies and directives under its control to incorporate the Board's standards.[6] The Board expects that the final standards and the revised Federal Acquisition Regulation will be issued at the same time.

Because of the delay in publishing the standards, the Board is considering making the standards effective six months after publication in the **Federal Register**. The Board believes that this action will provide Federal agencies with an opportunity to more fully understand these new requirements and will allow manufacturers of electronic and information technology time to ensure that their products comply with the standards. The Board also believes that this action is consistent with the Congressional intent underlying section 508. As discussed above, Congress provided a six month period between the publication of the Board's standards and the incorporation of the standards in the Federal Acquisition Regulation. This six month period would have allowed Federal agencies to understand the standards and manufacturers time to ensure that their products would be accessible.

*Question 1:* The Board seeks comment on the advisability of making the standards effective six months after publication in the **Federal Register.** This action would not affect the right of individuals with disabilities to file complaints for electronic and information technology procured after August 7, 2000 since that right is established by the statute.

Section 508(a)(4) provides that if a Federal agency determines that compliance with the standards imposes an undue burden, any documentation by the agency supporting a procurement shall explain why compliance creates an undue burden. Additionally, when it is determined that compliance with the standards imposes an undue burden, the Federal agency shall provide individuals with disabilities with the information and data involved by an alternative means of access that allows the individual to use the information and data.[7]

Section 508(a)(6)(A) states that when the Federal government provides access to the public to information or data through electronic and information technology, a Federal agency is not required to make equipment available or to purchase equipment at a location other than that where the electronic and information technology is provided to the public. Also, specific accessibility-related software or the attachment of specific accessibility-related peripheral devices are not required to be installed at workstations of Federal employees without disabilities.[8]

Section 508(c) provides that by February 7, 1999, each Federal agency shall evaluate the extent to which the electronic and information technology of the agency is accessible to and usable by individuals with disabilities and submit a report containing the evaluation to the Attorney General.

Section 508(d) provides that by February 7, 2000, the Attorney General shall prepare and submit to the President a report containing information on and recommendations regarding the extent to which the electronic and information technology of the Federal government is accessible to and usable by individuals with disabilities.[9] By August 7, 2001, and every two years thereafter, the Attorney General shall submit to the President and Congress a report containing information on and recommendations regarding the state of Federal agency compliance with the requirements of section 508, including actions regarding individual complaints.

Section 508(f) provides that beginning August 7, 2000, any individual with a disability may file a complaint alleging that a Federal agency fails to comply with section 508 in providing accessible electronic and information technology.[10] Complaints shall be filed with the Federal agency alleged to be in noncompliance. The Federal agency receiving the complaint shall apply the complaint procedures established to implement section 504 of the Rehabilitation Act for resolving

[4] The Clinger-Cohen Act was designed to ensure consistency across Federal agencies in the acquisition, use, and disposal of information technology. It requires each Executive agency to establish a process to select, manage, and evaluate the results of their information technology investments; report annually to Congress on progress made toward agency goals; and link information technology performance measures to agency programs.

[5] The Access Board is required to consult with the Secretary of Education, the Administrator of General Services, the Secretary of Commerce, the Chairman of the Federal Communications Commission, the Secretary of Defense, and the head of any other Federal agency that the Access Board determines to be appropriate.

[6] Whenever the Access Board revises its standards, the Council is required to revise the Federal Acquisition Regulation, and each appropriate Federal agency is required to revise its procurement policies and directives within six months to incorporate the revisions.

[7] Section 508(a)(1)(B).

[8] Section 508(a)(6)(B).

[9] On April 2, 1999, the Department of Justice (DOJ) released its self-evaluation materials for section 508. The self-evaluations were required to be submitted to the DOJ by June 15, 1999. The final report was not available prior to the publication of this proposed rule. It will be available through the Department of Justice Section 508 Home Page (http://www.usdoj.gov/crt/508/508home.html).

[10] This provision applies only to electronic and information technology that is procured by a Federal agency on or after August 7, 2000.

allegations of discrimination in a federally conducted program or activity. Under section 504, individuals may also sue an agency in Federal court to correct an alleged violation.

## Electronic and Information Technology Access Advisory Committee

This proposed rule is based on recommendations of the Electronic and Information Technology Access Advisory Committee (Committee or EITAAC). The Committee was convened by the Access Board in September 1998 to assist the Board in fulfilling its mandate under section 508.

On September 29, 1998, the Access Board published a notice appointing members to the Committee. 63 FR 51891 (September 29, 1998). Between October 1998 and May 1999, the Committee held 6 meetings, each of two working days in length, during which members worked to develop recommendations for implementing requirements under section 508. In selecting members of the Committee, the Access Board sought to ensure representation from all parties interested in the promulgation of electronic and information technology accessibility standards. The Committee was composed of representatives of the electronic and information technology industry; organizations representing the access needs of individuals with disabilities; and other persons affected by accessibility standards for electronic and information technology. Representatives of Federal agencies, including the departments of Commerce, Defense, Education, Justice, Veterans Affairs, the Federal Communications Commission, and the General Services Administration, served as ex-officio members or observers of the Committee. The following organizations served on the Committee:

American Council of the Blind
American Foundation for the Blind
Arkenstone, Inc.
Association of Access Engineering Specialists
Association of Tech Act Projects
Compaq
Easter Seals
Electronic Industries Alliance
FutureForms
Georgia Institute of Technology
IBM Special Needs Center
Information Technology Industries Council
Meeting the Challenge, Inc.
Microsoft Corporation
NCR Corporation
National Association of the Deaf
National Federation of the Blind
National Industries for the Blind
National Science Foundation
Pitney Bowes
Self Help for Hard of Hearing People, Inc.
Sun Microsystems
Trace Research and Development Center
United Cerebral Palsy Associations
WGBH National Center for Accessible Media
WebABLE! Solutions
World Wide Web Consortium, Web Accessibility Initiative

Each organization selected a principal member and an alternate. The Committee formed several subcommittees and task groups in which alternates and nonmembers were invited to participate. As a result, the actual group which developed the recommendations was broader than the formal membership. The result of the Committee's work was a report containing recommendations to the Access Board for implementing section 508 of the Rehabilitation Act Amendments of 1998. The Committee presented its report to the Board on May 12, 1999. This proposed rule is based primarily on the recommendations of chapters three ''Definitions'', four ''Section 508 Implementation'', and five ''Proposed Standards'' of the Committee report.

## Section-by-Section Analysis

This section of the preamble contains a concise summary of the rule which the Access Board is proposing. The text of the proposed rule follows this section.

### *Subpart A—General*

### Section 1194.1 Purpose

This section describes the purpose of the standards which is to implement section 508 of the Rehabilitation Act Amendments of 1998. The goal of section 508 is to introduce accessibility features into mainstream electronic and information technology products purchased by the Federal government to reduce the need for individual, customized accommodations and to make those accommodations which are still needed more efficient and easier to implement.

### Section 1194.2 Application

This section specifies what electronic and information technology is covered by the standards. Paragraph (a) states the general statutory requirement for electronic and information technology that must comply with the standards unless doing so would result in an undue burden. The term ''undue burden'' is defined at 1194.4, Definitions, and is discussed in the preamble under that section.

By statute, the enforcement provisions of section 508 apply only to products procured on or after August 7, 2000. (See section 508(f)(1)(B)). As a result, Section 508 does not authorize complaints or lawsuits to retrofit electronic and information technology products procured prior to August 7, 2000 to meet these standards. See a further discussion of the application of these standards to web sites maintained, developed, used or procured by the Federal government under 1194.23(c).

Paragraph (a)(1) states the statutory obligation of a Federal agency to make the information and data available by an alternative means when complying with the standards would result in an undue burden. For example, a Federal agency wishes to purchase a computer program that generates maps denoting regional demographics. If the agency determines that it would constitute an undue burden to purchase an accessible version of such a program, the agency would be required to make the information provided by the program available in an alternative means to users with disabilities. In addition, the requirements to make reasonable accommodations for the needs of an employee with a disability and to provide overall program accessibility under section 504 of the Rehabilitation Act also apply.

Paragraph (a)(2) sets forth the statutory requirement for an agency to document any claim of undue burden in a procurement. Such documentation must explain in detail which provision or provisions of this rule imposes an undue burden and the extent of such a burden. The agency should discuss each of the factors elaborated below which are to be considered an undue burden. By statute, the requirement to document an undue burden applies only to procurements.

Paragraph (b) applies this rule to electronic and information technology developed, procured, maintained, or used by an agency directly or used by a contractor pursuant to a contract with an agency. Consistent with section 5002(3)(C) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452) and as further discussed in 1194.3(b) below, products used by a contractor which are incidental to a contract are not covered by this rule. For example, a Federal agency enters into a contract to have a web site developed for the agency. The contractor uses its own office system to develop the web site. The web site is required to comply with this rule, however, the contractor's office system does not have to comply with these standards.

Paragraph (c) clarifies that procurement of products complying with this part is subject to commercial availability. That is, an agency is not expected to procure products that have not been developed. Documentation of an undue burden is not required in this case. This section also applies the provisions of this part to products that will be available in time to meet delivery requirements, or are developed by or on behalf of the government. This is based on existing provisions in the Federal Acquisition Regulations (see 48 CFR 2.101, Definitions of Words and Terms: Commercial item, paragraph (b)). For example, an agency may be planning a major software upgrade to be installed in the next year. If advances in technology or performance will be available to render the software compliant in time to meet the installation requirement, the product will be considered commercially available, despite the fact that a compliant version was not available at the time of the original solicitation. Of course, products developed in response to a Government solicitation are expected to be fully compliant.

The determination of commercial availability is to be applied on a provision by provision basis. That is, each provision is judged independently. Agencies cannot claim a product as a whole is not commercially available because it fails to meet some of the applicable provisions of these standards. It must still meet those provisions that are commercially available.

For example, some pagers may be available with a vibrating alert, but no model has voice output. A Federal agency would still be required to purchase the model with the vibrator even though a model with all the features necessary for accessibility may not exist. Similarly, if a software program that meets all of the provisions of 1194.23(b) is not available, but one that meets most of the provisions is (*e.g.*, it does not provide 8 foreground and 8 background colors), the agency must purchase that product that meets most of the applicable software provisions. The software program as a whole is not excused from the standards because a program meeting all of the provisions is not commercially available.

Paragraph (d) explains how each section of this rule is to be applied. In general, the requirements in 1194.21, 1194.23 and 1194.25 are assumed to satisfy the functional performance criteria in 1194.27. Therefore, when evaluating the compliance of any product, first look to compliance with 1194.21, 1194.23 and 1194.25, then apply the performance criteria in 1194.27 to elements or technologies not covered in those sections and to the overall product functions. Where there is overlap, the specific provisions in 1194.21, 1194.23 and 1194.25 prevail over the general provisions in 1194.27.

In developing these standards, the Board considered the issue of when accessibility features must be built-in and when the product need only be compatible, that is, have the ability to add on assistive technology or accessible features in the future as needed. Because the goal of section 508 is to introduce accessibility features into mainstream electronic and information technology, the proposed standards require that the accessibility features be built-in where reasonable and appropriate given the nature of the product and its intended use. For example, the standards require that the accessibility features be built-in for information kiosks because the public cannot be expected to attach an assistive technology device each time the kiosk is used. Because copy machines seldom allow for the loading of special software or the attachment of accessibility related peripherals, the standards require that the accessible features be built-in.

In general, where accessibility features are not built-in, the standards require that the system be compatible to make those accommodations which are still needed more efficient and easier to implement. For example, workstations are subject to the statutory exception that assistive technology devices are not required at workstations of persons without a disability. The standards require that these systems be compatible with the addition of assistive technology on an as needed basis.

The following paragraphs delineate those provisions where accessibility features are required to be built-in and those which permit compatibility in lieu of built-in features.

Section 1194.21 contains general requirements to be applied to all products, regardless of the specific technology involved. For example, the prohibition on using color coding exclusively is applicable to kiosks, web pages, copiers, software applications, or any other product that controls a visual display. The requirements in section 1194.21 pertain to built-in features.

Section 1194.23 provides requirements for specific components, such as keypads, software, web applications, and telecommunications. All but the simplest products will likely have more than one component and the requirements in section 1194.23 are to be applied to each component. For example, the keypad of a single line telephone can generally be made accessible to a person with a visual impairment by having a standard key layout and placing a nib on the five key. The keypad of a multi-line telephone can be made accessible in a similar fashion but the telephone may have visual indicators for availability of different lines and hold status. Each component for which there is a specific provision must be evaluated for compliance with this section.

The requirements in 1194.23(a), (d)(6)–(9), (e) and (f) are written to ensure built-in accessibility of keyboard, keypads and other mechanically operated controls, telecommunications equipment and information kiosks. The requirements in 1194.23(b), (c) and (d)(1)–(5) will ensure that software applications, web pages and certain telecommunications features are compatible with assistive technology.

Section 1194.25 provides requirements for compatibility of products with assistive technology commonly used by individuals with disabilities. Since any specific product cannot necessarily be made accessible to all disabilities, it must be able to accommodate assistive technology. For example, all computers are not expected to be equipped with a refreshable Braille display, but they are expected to be compatible with such equipment. Assistive technology may be part of a reasonable accommodation required by section 501 or section 504 of the Rehabilitation Act in response to a request made by a person with a disability.

Section 1194.27 provides functional performance criteria for overall product evaluation and for technologies or components for which there is no specific requirement under other sections. As in the example of the multi-line telephone discussed above, the keypad has specific requirements under section 1194.23, but the other functions, such as line availability or status, must be evaluated by applying the performance criteria. These criteria are also intended to ensure that the individual accessible components work together to create an accessible product. Section 1194.27(a), (b), (c) and (e) allow for the support of assistive technology to satisfy the criteria, whereas section 1194.27 (d) and (f) are functions that must be built into a product.

Finally, section 1194.31 provides requirements for information, documentation, and support. Products may meet all of the technical requirements of this part, but will not be usable to a person with a disability if information about the accessible features or how to use them is not available in a format the individual can use. Obviously, the format is critical to usability, since providing Braille to a person who does not read Braille is worthless, as is providing enhanced audio to a person who is deaf and does not rely on any residual hearing.

### Section 1194.3 General Exceptions

This section provides general exceptions from the standards. Paragraph (a) provides an exception for telecommunications or information systems operated by agencies, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or systems which are critical to the direct fulfillment of military or intelligence missions. This exception is statutory under section 508 and is consistent with a similar exception in section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452). This exception does not apply to a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). For example, software used for payroll, word processing software used for production of routine documents, ordinary telephones, copiers, fax machines, and web applications must still comply with the standards even if they are developed, procured, maintained, or used by an agency engaged in intelligence or military activities. On the other hand, a computer designed to provide early missile launch detection would not be subject to these standards.

Paragraph (b) provides an exception for electronic and information technology that is acquired by a contractor incidental to a Federal contract. That is, the products a contractor develops, procures, maintains, or uses which are not specified as part of a contract with a Federal agency are not required to comply with this part. For example, a consulting firm that enters into a contract with a Federal agency to produce a report is not required to procure accessible computers and word processing software to produce the report regardless of whether those products were used exclusively for the government contract or used on both government and non-government related activities. On the other hand, if such products were specified as contract deliverables (*i.e.*, they would become government property at the end of the contract) or if a Federal agency purchased the products to be used by the contractor as part of the project, those products would have to meet the standards. Similarly, if a firm is contracted to develop a web site for a Federal agency, the web site created must be fully compliant with this part, but the firm's own web site would not be covered. This exception is consistent with a similar exception in section 5002(3)(C) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).

Paragraph (c) clarifies that, except as required to comply with these standards, this part does not require the installation of specific accessibility-related software or the attachment of an assistive technology device at a workstation of a Federal employee who is not an individual with a disability. Specific accessibility related software means software which has the sole function of increasing accessibility for persons with disabilities to other software programs (*e.g.*, screen magnification software). The purpose of section 508 and these standards is to build as much accessibility as is reasonably possible into general products developed, procured, maintained, or used by agencies. However, it is not expected that every computer will be equipped with a refreshable Braille display, or that every software program will have a built-in screen reader. Such assistive technology may be required as part of a reasonable accommodation for an employee with a disability or to provide program accessibility. To the extent that such technology is necessary, products covered by this part must not interfere with the operation of the assistive technology.

Paragraph (d) specifies that when agencies provide access to information or data to the public through electronic and information technology, agencies are not required to make equipment owned by the agency available for access and use by individuals with disabilities at a location other than that where the electronic and information technology is provided to the public, or to purchase equipment for access and use by individuals with disabilities at a location other than that where the electronic and information technology is provided to the public. For example, if an agency provides an information kiosk in a Post Office, a means to access the kiosk information for a person with a disability need not be provided in any location other than at the kiosk itself.

Paragraph (e) states that compliance with this part does not require a fundamental alteration in the nature of a product or its components. Fundamental alteration means a change in the fundamental characteristic of the product, not merely a cosmetic or aesthetic change. For example, an agency intends to procure pocket-sized pagers for their field agents. Adding a large display to a small pager may fundamentally alter the device by significantly changing its size to such an extent that it no longer meets the purpose for which it was intended, that is to fit in a shirt or jacket pocket.

### Section 1194.4 Definitions

*Accessible*: The term accessible is defined in terms of compliance with the standards in this part, as is common with other accessibility standards. That is, if a product complies with the standards in this part, it is accessible; if it does not comply, it is not accessible.

*Agency:* Section 508 applies to any Federal department or agency, including the United States Postal Service (section 508(a)(1)(A)). The term ''agency'' as used in this rule includes all of these entities.[11]

*Alternate Formats and Alternate Modes:* These terms are given the same meaning here as in the Board's Telecommunications Act Accessibility Guidelines (36 CFR part 1193). Certain product information is required to be made available in alternate formats to be usable by individuals with various disabilities. Common forms of alternate formats are Braille, large print, ASCII text, and audio cassettes. Alternate modes are different means of providing information to users of products including product documentation and information about the status or operation of controls. For example, if product instructions are provided on a video cassette, captioning would be required.

*Assistive Technology:* Assistive technology means any item, piece of equipment, or system, whether acquired commercially, modified, or customized, that is commonly used to increase, maintain, or improve functional capabilities of individuals with disabilities. The definition is derived from a definition of assistive technology in the Assistive Technology Act of 1998 (29 U.S.C. 3001 *et seq.*).

Examples of assistive technology include, but are not limited to, (1) Screen readers which allow persons who cannot see a visual display to either hear screen content or read the content in Braille; (2) a specialized one-handed keyboard which allows an individual to operate a computer with only one hand; and (3) specialized audio amplifiers that allow persons with limited hearing to receive an enhanced audio signal.

[11] A government depository library is not considered a Federal agency.

*Electronic and Information Technology:* This is the statutory term for the products intended to be covered by the standards in this part. The statute explicitly required the Board to define this term, and required that the definition be consistent with the definition of ''information technology'' in the Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)). Therefore, this definition includes information technology as defined by that Act, as well as any equipment or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information.

Electronic and information technology includes, but is not limited to, telecommunications products (such as telephones), information kiosks and transaction machines, web sites, multimedia, and office equipment such as copiers and fax machines. Consistent with the Federal Acquisition Regulations,[12] electronic and information technology does not include any equipment that contains imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

*Information Technology:* The definition of information technology is the same as the definition of information technology in section 5002(3) of the Clinger-Cohen Act. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

*Operable Controls:* Operable controls are those components of a product that require manipulation or contact for operation of the device. Controls include on/off switches, buttons, dials and knobs, mice, keypads and other input devices, copier paper trays (both for inserting paper to be copied and retrieving finished copies), coin and card slots, card readers, and similar components. Operable controls do not include voice-operated controls.

*Product:* Product is used as a shorthand for electronic and information technology throughout this part.

*TTY:* The term TTY is defined to be consistent with the Board's ADA Accessibility Guidelines (36 CFR part 1191) and Telecommunications Act Accessibility Guidelines.

*Telecommunications:* This term is defined consistent with the Board's Telecommunications Act Accessibility Guidelines and the definition of telecommunications in the Telecommunications Act (47 U.S.C. 153).

*Undue Burden:* The term ''undue burden'' is based on caselaw interpreting section 504 of the Rehabilitation Act (*Southeastern Community College* v. *Davis,* 442 U.S. 397 (1979)), and has been included in agency regulations issued under section 504 since the *Davis* case. See, *e.g.,* 28 CFR 39.150. The term ''undue burden'' is also used in Title III of the Americans with Disabilities Act. (ADA), 42 U.S.C. 12182(b)(2)(A)(iii). The legislative history of the ADA states that the term ''undue burden'' is derived from section 504 and the regulations thereunder, and is analogous to the term ''undue hardship'' in Title I of the ADA, which Congress defined as ''an action requiring significant difficulty or expense.'' 42 U.S.C. 12111(10)(A). See, H. Rept. 101–485, pt. 2, at 106. The Board has adopted this definition for ''undue burden.''

Title I of the ADA lists factors to be considered in determining whether a particular action would result in an undue hardship. 42 U.S.C. 12111(10)(B)(i)–(iv). Since Title I of the ADA addresses employment, not all of the factors are directly applicable to section 508 except for the financial resources of the covered facility or entity. In determining whether a particular action is an undue burden under section 508, the rule provides that the resources available to an agency or component for which the product is being developed, procured, maintained, or used is a factor to be considered. An agency's entire budget may not be available for purposes of complying with section 508. Many parts of agency budgets are authorized for specific purposes, and/or are provided as grants to non-Federal entities, and are thus not available for other purposes. Because available financial resources vary greatly from one agency to another, what constitutes an undue burden for a smaller agency may not be an undue burden for another, larger agency having more resources to commit to a particular procurement. Each procurement would necessarily be determined on a case-by-case basis.

The Board is considering including two additional factors in the final rule to determine whether an action is an undue burden.

*Factor (2):* An agency may consider the extent to which a product meeting the standards is compatible with the agency's or component's technology infrastructure, including security, and the difficulty of integrating the accessible product. For example, an agency wishes to contract with a digital cellular provider in order to provide cellular phone service to its employees. The agency's digital cellular network is not compatible with TTYs. Since these two products are incompatible with each other, it will result in an undue burden. The agency would not be prohibited from contracting with the digital provider. However, accommodations for TTY users could be made through an analog cellular phone, if needed. Should compatibility become feasible over time, this no longer would be viewed as an undue burden.

*Factor (3):* An agency may also consider the functionality needed from the product and the technical difficulty involved in making such a product accessible. For example, an agency needs to purchase a computer assisted design (CAD) software program. The function of the CAD program is to produce visual drawings. Technology is available to produce basic tactile images usable by an employee with a visual impairment, but to apply this technology to a CAD program would be extraordinarily difficult and have limited functionality, making it an undue burden.

*Question 2:* The Board seeks comment on whether factors (2) and (3) discussed above are appropriate factors for consideration in determining whether an action would be an undue burden under these standards.

### Section 1194.5 Equivalent Facilitation

This section allows the use of designs or technologies as alternatives to those prescribed in this part provided that they result in substantially equivalent or greater access to and use of a product for people with disabilities. This provision is not a ''waiver'' or ''variance'' from the requirement to provide accessibility, but a recognition that future technologies may be developed, or existing technologies could be used in a particular way, that could provide the same functional access in ways not envisioned by these standards. In evaluating whether a technology results in ''substantially equivalent or greater access,'' it is the functional outcome,

[12] 48 CFR Chapter 1, part 2, section 2.101 Definitions Information Technology (c).

not the form, which is important. For example, an information kiosk which is not accessible to a person who is blind might be made accessible by having a telephone handset that connects to a computer that responds to touch-tone commands and delivers the same information audibly.

### *Subpart B—Accessibility Standards*

This proposed rule is based primarily on the recommendations of chapter five of the EITAAC report. The proposed rule rearranges and renames sections from the EITAAC report. Although the Board has reorganized the committee's recommendations, the Board believes that the concepts and most of the committee's recommended requirements have been preserved. The generic standards (EITAAC 5.2) are now labeled as functional performance criteria (1194.27). The Board made this change because it believes this group of specifications are yardsticks to use to measure performance as opposed to objective standards. Section 1194.27 contains the functional performance criteria against which all products will be judged. Sections 1194.23 and 1194.25 are the component specific and compatibility standards for accessibility. Where the Board has not included a recommendation from the committee's report it is noted.

### Section 1194.21—General Requirements

The requirements under this section are general, because they do not apply to any specific product. For example, the requirements relating to displays apply to any display whether on a computer, a copier, or information kiosk and transaction machine.

*Question 3:* The Board seeks comment on the current organization of sections 1194.21 and 1194.23. Other ways of organizing functions may be more appropriate. The Board seeks comment on other approaches to organizing functions and requirements that might be easier to understand and implement.

Paragraph (a) provides that color coding shall not be used as the only means of identifying a visual element. This requirement applies to all products, whether web based or free standing office equipment. Relying on color as a singular method for identifying screen elements or controls poses serious problems, not only for people with limited or no vision, but also for those who are color blind. This requirement does not prohibit the use of color to help with component identification. It does however, require that some other method of identification, such as text labels, be combined with the use of color. While this provision is consistent with the recommendations of the advisory committee, the committee also recommended including a similar functional performance requirement. The functional performance criterion was not included in the proposed standards as it was duplicative of this requirement.

Paragraph (b) provides provisions for the physical characteristics of large office equipment including reach ranges and the general physical accessibility of controls and features. A large, free standing copier would be an example of a product addressed by this provision. This requirement is consistent with the recommendations of the advisory committee and is based on the Americans with Disabilities Act Accessibility Guidelines (ADAAG 4.2 Space Allowance and Reach Ranges). Two figures are provided to help explain the application of the provision.

Paragraph (c) provides that flashing visual displays and indicators shall not exceed a frequency of two Hertz. In 1988, the Board sponsored two research projects on visual fire alarms that found that individuals with photosensitive epilepsy can have a seizure triggered by displays which flicker or flash, particularly if the flash has a high intensity and is within certain frequency ranges. This provision limits the frequency of flashing visual displays and indicators to avoid triggering a seizure in an individual with photosensitive epilepsy. This requirement is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (d) provides that where a timed response is required, at least one mode which does not require users to respond within a timed interval shall be provided; or at least one mode which allows users to adjust the response times to at least 5 times the default setting shall be provided. Requiring a user to respond within a certain length of time is a method commonly used by interactive menu driven systems. If a person is calling through a telephone relay service, or has a dexterity related disability, entering information such as a social security number within a specified time may be difficult or impossible. This provision is consistent with the recommendations of the advisory committee.

*Question 4:* The Board seeks information on whether a system is commercially available that would allow an individual user to adjust the response time interval, and if so, whether 5 times the default setting is the correct standard. If available, what is the cost of such a system? The Board is also interested in comments addressing any security concerns raised by this requirement. For example, would the security of an information kiosk which allowed individuals to access personal information be compromised by allowing for the adjustment of the time-out feature?

Paragraph (e) provides that where biometric forms of user identification or activation are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided. Identification by biometric forms such as retina scan, fingerprint or palm print are growing in popularity. They are used for building access as well as electronic system access. However, such identification measures create access problems for some persons with disabilities. For example, if a system relies on fingerprint identification for access, a person with prosthetic hands would not be able to use the system. As a result, the Board is proposing to require that an alternative form of identification be provided which does not rely on particular biological characteristics. Under section 504 of the Rehabilitation Act, an employee who is unable to access a system due to the constraints of a biological characteristic may be entitled to a reasonable accommodation which would enable him or her to access the system through an alternative measure. This provision would require that an alternative measure be in place when the system is procured. This requirement is consistent with the recommendations of the advisory committee.

*Question 5:* The Board may consider requiring multiple forms of biological identification as an alternative to requiring non-biological identification in the final rule. Would this be a better solution? What would be the cost impact of requiring multiple forms of biological identification? Does requiring an alternative mode of identification which is not based on biological characteristics lessen security? The proposed standards require that an alternative form of identification be built-in whenever biometric identification is used. The Board is seeking comment on whether the final rule should permit the alternative method of identification to be added on at a later date rather than built-in at the time of procurement. If so, should compatibility be limited to workstations or to all systems that use biometric identification?

Paragraph (f) requires touchscreen and touch-operated controls to be operable without requiring body contact or close body proximity. This requirement addresses the difficulty that individuals who have artificial hands or use headsticks or mouthsticks to operate products have with capacitive or heat-operated controls which require contact with a person's body. Touch-operated is not the same as a control which is operated by pushing a button or sliding a switch. Touch-operated controls are activated by merely touching them or placing a body part, usually a finger, in very close proximity. They often depend on the body acting as an electrical conductor which changes the capacitance of the switch. In addition, some touch operated controls are designed to detect the heat from a finger. In both of these instances, the control cannot be activated by a prosthetic limb, a mouthstick, or even a gloved hand.

Alternative access modes which do not require body contact or close body proximity may include keypad input and voice input and different types of touchscreens or touch-operated controls which do not require bodily contact or proximity to operate. This provision is consistent with the recommendations of the advisory committee.

Section 1194.23 Component Specific Requirements

The requirements in the following paragraphs address specific components of products. Paragraph (a) applies to mechanically operated controls, keyboards or keypads. These provisions address controls which require a user to physically manipulate or press a switch, button, or knob, to operate a product.

Paragraph (a)(1) provides that controls and keys shall be tactilely discernible without activating the controls or keys. Tactilely discernible means that individual keys can be located and distinguished from adjacent keys. To comply with this requirement, controls that must be touched to activate, must be distinguishable from each other. This can be accomplished by using various shapes, spacing, or tactile markings. Because touch is necessary to discern tactile features, this provision provides that the control should not be activated by mere touching. For example, the standard desktop computer keyboard would meet this requirement because the tactile mark on the ''j'' and ''f'' keys permits a user to locate all other keys tactilely. The geographic spacing of the function, ''numpad'' and cursor keys make them easy to locate by touch. In addition, most keyboards require some pressure before they transmit a keystroke. Conversely, ''capacitance'' keyboards that react as soon as they are touched and have no raised marks or actual keys would not meet this requirement. A ''membrane'' keypad with keys that must be pressed can be made tactilely discernible by separating keys with raised ridges so that individual keys can be distinguished by touch. This provision is consistent with the recommendations of the advisory committee.

Paragraph (a)(2) provides that the status of toggle controls such as the ''caps lock'' or ''scroll lock'' keys be determined by both visual means and by touch or sound. For example, adding audio patterns such as ascending and descending pitch tones that indicate when a control is turned on or off would alleviate the problem of a person who is blind inadvertently pressing the locking or toggle controls. Also, buttons which remain depressed when activated or switches with distinct positions would meet this provision. This provision is consistent with the recommendations of the advisory committee.

Paragraph (a)(3) provides that controls shall be accessible to persons with limited dexterity. Individuals with tremor, cerebral palsy, paralysis, arthritis, or artificial hands may have difficulty operating systems which require fine motor control, assume a steady hand, or require two hands or fingers to be used simultaneously for operation. Individuals with high spinal cord injuries, arthritis, and other conditions may have difficulty operating controls which require significant strength. The provision limits the force required to five pounds and is based on section 4.27.4 of the ADA Accessibility Guidelines and is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (a)(4) provides that access to all program functions shall be available through keyboard or keypad commands. Keyboard or keypad commands provide a viable alternative for those who cannot use a pointing device or touchscreen. This provision does not require that every product have a keyboard. It requires that where a keyboard or keypad is provided, the program functions shall be available through keyboard or keypad commands. This provision is consistent with the recommendations of the advisory committee.

Paragraph (a)(5) establishes requirements for key repeat rate where an adjustable keyboard repeat rate is supported. It requires that the keyboard delay before repeat shall be adjustable to at least two seconds per character. This provision is consistent with the recommendations of the advisory committee.

The advisory committee also recommended three provisions that the Board has not included in this proposed rule. The committee recommended that assigned keyboard access (e.g., Ctrl+P for Print, Escape for cancel) be provided for commonly used functions or commands and that the keyboard map not change except under user control, so that a user memorizing key locations shall be able to rely on those locations. The Board has not included these provisions since they are user convenience issues not accessibility issues. The committee also recommended that all keyboard access functionality be documented with a product or follow documented operating system conventions. This provision is not included since documentation is already addressed by section 1194.31.

Paragraph (b) applies to non-embedded software applications and operating systems. All electronic and information technology products operate by following programming instructions referred to as software. Software can be divided into two broad categories: software that is embedded in a chip mounted in a product and software that is loaded onto a storage device such as a hard disk and can be erased, replaced or updated. The provisions in this section address requirements for accessible ''installable, non-embedded'' software.

Paragraph (b)(1) requires the use of keystrokes for navigation among interface elements. For persons with vision impairments who cannot use a pointing device such as a mouse, having access to program controls through keyboard navigation is essential. An example of this feature would be the ability to tab through the choices in a dialog box rather than requiring that a user move a pointer to a particular selection and click on it. This provision is consistent with the recommendations of the advisory committee.

Paragraph (b)(2) prohibits applications from disabling access features of applications or the operating system. There are commercially available software applications and operating systems that have accessibility features built-in that can be turned on or off by a user. These include features that can reverse the color scheme, show an image when an error tone is generated, or provide for ''sticky keys'' that allow a user to hit key combinations (such as control-C) sequentially rather than simultaneously. This provision prohibits other software programs from disabling these features when selected. This requirement is consistent with the recommendations of the advisory committee.

Paragraph (b)(3) requires that a well-defined on-screen indication of the current focus be provided that moves among interactive interface elements as the input focus changes. The focus is the point on a screen where an action will occur when a keystroke or mouse click is activated. For example, when an individual displays a file directory on the screen, the focus point shows what file will be activated when the enter key is pressed. The focus must be programmatically exposed so that assistive technology can track the focus and focus changes and be easily seen by the user. The focus point must be identified in the program language. Making the identification of the focus point in the software programmatically available allows programmers of assistive technology software such as screen readers, to let the user know where the current focus is placed. This provision is consistent with the recommendations of the advisory committee.

Paragraph (b)(4) requires that programs provide sufficient information about a user interface element, including the identity, operation and state of the element, to assistive technology software. User interface elements can include, but are not limited to, buttons, checkboxes, menu bars, or tool bars. For assistive technology to operate efficiently, it must have access to the information about a user interface from the program to be able to inform the user of the existence, location, and status of all interface elements. This provision is consistent with the recommendations of the advisory committee.

Paragraph (b)(5) provides requirements for accessing images that represent an action. For example, a push button, checkbox or other action point is often represented by a graphic. Assistive technology however, cannot describe pictures or graphics. This provision requires that programs provide text such as a ''tooltip'' for the assistive technology to interpret the pictures so that a user of assistive technology can identify what action will occur when an element is activated by a keystroke or mouse click. This provision is consistent with the recommendations of the advisory committee.

Paragraph (b)(6) provides that the use of an image will be consistent throughout an application. Most screen reading programs allow users to assign text names to bitmap images. If the bitmap image should change meaning during the running of an application, the assigned identifier is no longer valid. This provision prohibits the changing of the meaning of a bitmap image during an application and is consistent with the recommendations of the advisory committee.

Paragraph (b)(7) provides that software must follow standard programming techniques applicable for the specific operating system when software programs supply text to assistive technology programs. If programs are written using nonstandard code, other programs such as software for assistive technology may not be able to receive information from the application. At a minimum, the types of text information that must be available include text content, text input caret location, and text attributes. This provision is consistent with the recommendations of the advisory committee.

Paragraph (b)(8) requires that a minimum of eight foreground and eight background color selections capable of producing a variety of contrast levels be provided. This provision requires more than just providing color choices. The available choices must also allow for different levels of contrast. Many people experience a high degree of sensitivity to bright displays. Someone with this condition cannot focus on a bright screen for long because they will soon be unable to distinguish individual letters. An overly bright background causes a visual ''white-out''. To alleviate this problem, the user must be able to select a softer background and appropriate foreground colors.

In addition to requiring different levels of colors and contrasts, the advisory committee recommended providing a ''wide variety'' of font size and style settings. The proposed provision does not require variations of font sizes and styles because those who would benefit from increased font size will also need an increase in the size of all screen elements. This can best be accomplished by adding screen enlargement software to the system.

*Question 6:* The Board seeks comment on whether eight foreground and eight background colors is sufficient to give the user ample selections. If a larger number of choices were required, is software commercially available from more than one manufacturer?

Paragraph (b)(9) prohibits applications from overriding user selected contrast and color selections. This provision addresses the problem of applications refusing to respect system-wide settings and is consistent with the recommendations of the advisory committee. Often persons with disabilities prefer to select color, contrast, keyboard repeat rate, and keyboard sensitivity settings in an operating system. When an application disables these settings, accessibility is reduced. This provision allows the user to select personalized settings which cannot be disabled by software programs.

Paragraph (b)(10) requires that people with disabilities have access to electronic forms. Electronic forms are a popular method used by many agencies to gather information or permit a person to apply for services, benefits, or employment. The 1998 Government Paperwork Elimination Act requires that Federal agencies make electronic versions of their forms available online and allows individuals and business to use electronic signatures to file these forms electronically. This provision requires that when an agency uses a form that cannot be read and manipulated by assistive technology, an alternative form must also be provided that is accessible. An example of a form which is not accessible is one which is graphical in nature and cannot be translated into meaningful text by assistive technology. This provision is consistent with the recommendations of the advisory committee.

Paragraph (b)(11) establishes requirements for handling animated text. The use of animation on a screen can pose serious access problems for users of screen readers or other assistive technology. When important elements such as push buttons or relevant text are animated, the user of assistive technology cannot access the application. This provision requires that in addition to the animation, an application provide the elements in a static form. This provision is consistent with the recommendations of the advisory committee.

The advisory committee also recommended that system startup and restart be accessible, however, the Board has not included that provision in the proposed rule since no measurable standards were recommended.

Paragraph (c) applies to web-based information and applications. These standards do not apply to external web sites, including search engines, which are not developed or procured by a Federal agency. For example, an employee of an agency may use a search engine which is based on a commercial web site. That search engine does not have to comply with these standards.

By statute, when a Federal agency develops, procures, maintains or uses electronic and information technology, including web-based information and applications, they must comply with these standards unless to do so would be an undue burden (section 508(a)(1)(A)). The enforcement provisions of section 508, however, are limited to those web-based information and applications that are procured on or after August 7, 2000. (See section 508(f)(1)(B)). The enforcement provisions are silent with respect to products which are not procured, but are developed, used or maintained by a Federal agency (*e.g.,* an agency develops a web page in house). However, even though the enforcement mechanisms provided in section 508 do not authorize complaints or lawsuits for inaccessible products which are developed, used or maintained by an agency, the Board expects that these products, including web pages, will be accessible. (See section 508(a)(1)(A) which addresses the development, procurement, maintenance, or use of electronic and information technology by the Federal government.) The Board notes that section 504 of the Rehabilitation Act imposes a duty on the Federal government to make programs conducted by the Federal government (*e.g.,* an agency web site) accessible and that both sections 501 and 504 of that Act requires that Federal agencies address the needs of employees with disabilities. (29 U.S.C. 794 (section 504); 29 U.S.C. 791 (section 501)). It is possible that in determining compliance with these statutory obligations, the standards issued by the Board under section 508 of the Rehabilitation Act will be used as a yardstick to measure whether a program is accessible. Furthermore, under section 508 of the Rehabilitation Act, the Department of Justice has an obligation to prepare biennial reports assessing compliance by Federal agencies with these standards (section 508(d)(2)). That report would address products developed, procured, maintained or used by the Federal government, as well as actions regarding individual complaints.

*Example 1:* On January 1, 2001, a Federal agency enters into a procurement contract with an outside entity for the development of an agency web site. That web site would have to meet these standards, unless to do so would be an undue burden. Because it is a procurement on or after August 7, 2000, the agency would be subject to a complaint or civil action if the web site was not accessible. Suppose however, the agency develops its own web site. That web site would have to be accessible under section 508(a)(1)(A), unless it was an undue burden, but because it was not a procurement, the enforcement provisions under section 508(f) of the Rehabilitation Act would not apply. While there may not be a remedy under section 508, there would be recourse under section 504 of the Rehabilitation Act in that the agency was conducting a program that was not accessible.

*Example 2:* An agency has an existing web site and enters into a procurement contract with an outside entity to develop new pages to be added to its web site to address a new program. The content of the new pages would have to meet these standards unless to do so would be an undue burden. If the procurement was on or after August 7, 2000, the accessibility of the new pages could be the subject of a complaint or civil action. With respect to the preexisting web site, it would be subject to the agency's obligations under section 504 of the Rehabilitation Act which may require that the agency develop a plan to update the web site and make it accessible over a period of time.

The advisory committee recommended that the Board's standards reference the World Wide Web Consortium's (W3C) Web Accessibility Initiative's (WAI)[13] Web Content Accessibility Guidelines, User Agent Accessibility Guidelines, and Authoring Tool Accessibility Guidelines, including requirements from priority levels one and two for each document.

Rather than referencing the WAI guidelines, the proposed standards include provisions which are based generally on priority level one checkpoints of the Web Content Accessibility Guidelines 1.0, as well as other agency documents on web accessibility and additional recommendations of the advisory committee. The Board's rephrasing of language from the Web Content Accessibility Guidelines 1.0 in paragraph (c) of the proposed rule has not been reviewed by the W3C, since proposed rules are not made public until published in the **Federal Register**.

The advisory committee also included specific recommendations for browsers and web authoring tools. Because web browsers and web authoring tools, (as well as web pages) are software in nature, they must also comply with the requirements of section 1194.23(b).

Paragraph (c)(1) requires that a text equivalent be provided for every non-text element. For example, a link or graphic on a web page that indicates an action or a URL cannot be interpreted by assistive technology. This provision would require that an alternative text label be assigned to that link or graphic. This provision is consistent with the recommendations of the advisory committee.

Paragraph (c)(2) requires alternatives for color based prompting. The creative use of color can enhance the look of web pages. However, a person who has either low vision or is color blind would have difficulty activating color based prompts. Web pages therefore, are required to indicate with text that which is evident by using color. For example, a statement such as ''press the green button to begin,'' should read ''press the green button labeled start to begin,'' and the word ''start'' should be associated with the green button. This provision is consistent with the recommendations of the advisory committee.

Paragraph (c)(3) provides that the user be alerted to a change in the natural language of a web page. For example, this requirement can be met by adding a line of text to a web page which changes from English to French by adding text which reads ''the following paragraph is presented in French.'' Most screen readers used by blind and visually impaired persons only have rules for pronouncing one language. If the web site did not alert the user to a language change, the user would be at a loss as to why the page had become unintelligible. This provision is consistent with the recommendations of the advisory committee.

Paragraph (c)(4) provides that documents must be organized so they are readable without requiring style sheets. Style sheets are a relatively new technology that allows web site designers to easily control formatting (such as font size and color and text alignment) throughout their web pages. This provision does not prohibit the use of style sheets (which can often be used to enhance accessibility) provided that web pages using style sheets can be viewed by browsers not supporting style sheets and by browsers that have disabled support for style sheets. In addition, certain newer browsers allow users to define their own style sheets to improve the accessibility of web pages. This provision prohibits the use of style sheets that interfere with user defined style sheets. This provision is consistent with the recommendations of the advisory committee.

Paragraph (c)(5) requires that when alternative access to web page content, such as captioning of audio programs or multimedia, is provided, that alternative

[13] The Web Accessibility Initiative (WAI), in coordination with organizations around the world, is pursuing accessibility of the web through five primary areas of work: technology, guidelines, tools, education and outreach, and research and development. Additional resources are available at http://www.w3.org/WAI, including the Web Content Accessibility Guidelines 1.0, available at http://www.w3.org/TR/WCAG10.

must be updated on the screen every time the content changes. This provision is consistent with the recommendations of the advisory committee.

Paragraph (c)(6) provides that redundant text links must be provided for each active region of a server-side image map. When a web page uses server-side maps as navigation aids, the individual browser cannot communicate the URL that will be followed when a region of the map is activated. Therefore, the redundant text link will be necessary to provide access to the page for anyone not able to see or load the map. This provision is consistent with the recommendations of the advisory committee.

Paragraph (c)(7) provides that client-side image maps must be used whenever possible in place of server-side image maps. When a web page downloads a client-side image map to a browser, it also sends all the information about what action will happen when a region of the map is pressed. For this reason, client-side image maps, even though graphical in nature, will show the links related to the map in a text format. This provision is consistent with the recommendations of the advisory committee.

Paragraphs (c)(8) and (9) permit the use of tables, but require that the tables be coded according to proper HTML rules. Many assistive technology applications can interpret the HTML coding of tables. When tables are coded inaccurately or table codes are used for non tabular material, the assistive technology cannot accurately read the content.

Paragraph (c)(10) establishes requirements for the use of frames. Frames can be an asset to users of screen readers if the labels on the frames are explicit. Such labels as top, bottom, or left, provide few clues as to what is contained in the frame. Labels such as ‘‘navigation bar’’ or ‘‘main content’’ are more meaningful and facilitate frame identification and navigation. This provision is consistent with the recommendations of the advisory committee.

Paragraph (c)(11) provides that scripts, applets, or other plug-ins must not be essential to reading or navigating a web page. When the content or navigation of a web page relies on scripts or requires that a user have a specific plug-in installed, the result can be an inaccessible page. If the page cannot be created with text attributes for navigation and content that do not require a plug-in, then an alternate text page may be the only solution. The Board recommends that access features be incorporated into all web pages without resorting to alternative text pages. This provision is consistent with the recommendations of the advisory committee.

Paragraph (c)(12) provides that when features such as captioning for audio output or descriptive audio for graphics is provided, the captioning or description must be presented in a synchronous manner. This provision is consistent with the recommendations of the advisory committee.

Paragraph (c)(13) provides that an appropriate method must be used to facilitate the easy tracking of page content that provides users of assistive technology the option to skip repetitive navigation links. It is common for web authors to place navigation links at the top, bottom, or side of every new page. This technique can render use of a web site very difficult for persons using a screen reader as screen readers move through pages reading from top to bottom. The use of repetitive navigation links forces persons with visual impairments to re-read these links when moving to every new page. This provision allows the user to more efficiently read the contents of a page. This provision is consistent with the recommendations of the advisory committee.

The advisory committee also recommended that if extensive ASCII art is used, a link should be provided to allow a user to jump to the end of the ASCII art. The Board has not included this provision since it is a user convenience issue not an accessibility issue.

Paragraph (d) applies to telecommunications functions. These provisions address products which involve the transmission of information without changing the form or content of the information as sent and received. ‘‘Telecommunications’’ is further defined in section 1194.4, Definitions.

Paragraph (d)(1) requires that products shall provide a standard non-acoustic connection point for TTYs when they have a function that allows voice communication and do not provide a TTY functionality. It shall also be possible for the user to easily turn any microphone on the product on and off to enable the user who can talk to intermix speech with TTY use. Individuals who use TTYs to communicate must have a non-acoustic way to connect TTYs to telephones in order to obtain clear TTY connections, such as through a direct RJ–11 connector, a 2.5 mm audio jack, or automatic switching. When a TTY is connected directly into the network, it must be possible to turn off the acoustic pickup (microphone) to avoid having background noise in a noisy environment mixed with the TTY signal. Since some TTY users make use of speech for outgoing communications, the microphone on/off switch must be easy to flip back and forth or a push-to-talk mode should be available. This provision is consistent with the Board’s Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (d)(2) requires products providing voice communication functionality to be able to support use of all cross-manufacturer non-proprietary standard signals used by TTYs. Some products compress the audio signal in such a manner that standard signals used by TTYs are distorted or attenuated, preventing successful TTY communication. Use of such technology is not prohibited as long as the compression can be turned off to allow undistorted TTY communication. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (d)(3) provides that voice mail, auto-attendant, and interactive voice response telecommunications systems shall be usable by TTY users with their TTYs. Voice mail systems are available which allow TTY users to retrieve and leave TTY messages. This provision does not require that phone systems have voice to text conversion capabilities so that a person who is deaf can retrieve a voice mail message directly with their TTY without relying on a relay service or an interpreter, but it does require that TTY users can retrieve and leave TTY messages. This provision is consistent with the recommendations of the advisory committee.

Paragraph (d)(4) prohibits telecommunications services, such as interactive systems, from imposing time limits for responses. For example, a person accessing a Federal agency’s automated menu from a TTY may need additional time to read the options and respond. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (d)(5) provides that functions such as caller identification must be accessible for users of TTYs, telecommunications relay services, and for users who cannot see displays. This provision is consistent with the recommendations of the advisory committee.

Paragraph (d)(6) requires products to be equipped with volume control that provides an adjustable amplification up to a minimum of 20 dB of gain. If a volume adjustment is provided that allows a user to set the level anywhere from 0 to the upper requirement of 20 dB, there is no need to specify a lower limit. If a stepped volume control is provided, one of the intermediate levels must provide 12 dB of gain. The gain applies to the voice output not Baudot, ASCII, or other machine codes. The proposed level of amplification is different from that required under the Hearing Aid Compatibility Act and the Federal Communications Commission's (FCC) regulations (47 CFR 68.317 (a)). The FCC requires volume control that provides, through the receiver in the handset or headset of the telephone, 12 dB of gain minimum and up to 18 dB of gain maximum, when measured in terms of Receive Objective Loudness Rating.

In accordance with the National Technology Transfer and Advancement Act, this provision is consistent with the 1998 ANSI A117.1 document, ''Accessible and Usable Buildings and Facilities.'' ANSI is the voluntary standard-setting body which issues accessibility standards used by the nation's model building codes. The Board has issued a separate NPRM to harmonize the existing ADAAG provision with the ANSI standard. This provision is consistent with the Telecommunications Act Accessibility Guidelines. Tests conducted by two independent laboratories found high gain phones without special circuitry currently on the market which had 90 dB and 105 dB at maximum volume setting. This is a 20 dB gain over the standard 85 dB ambient noise level. (See Harry Teder Ph.D., Consulting in Hearing Technology; Harry Levitt, Ph.D., Director, Rehabilitation Engineering and Research Center on Hearing Enhancement and Assistive Devices, Lexington Center).

Paragraph (d)(7) requires that an automatic reset be installed on any telephone that allows the user to adjust the volume higher then the normal level. This is a safety feature to protect people from suffering damage to their hearing if they accidentally answer a telephone with the volume turned too high. This provision is consistent with the recommendations of the advisory committee.

Paragraph (d)(8) requires products that provide auditory output by an audio transducer normally held up to the ear, to provide a means for effective wireless coupling to hearing aids. Generally, this means the earpiece generates sufficient magnetic field strength to induce an appropriate field in a hearing aid T-coil. The output in this case is the direct voice output of the transmission source, not the ''machine language'' such as tonal codes transmitted by TTYs. For example, a telephone must generate a magnetic output so that the hearing aid equipped with a T-coil can accurately receive the message. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (d)(9) requires that interference to hearing technologies shall be reduced to the lowest possible level that allows a user of hearing technologies to utilize a telecommunications product. Individuals who are hard of hearing use hearing aids and other assistive listening devices, but they cannot be used if products introduce noise into the listening aids because of electromagnetic interference. The American National Standards Institutes (ANSI) has established a task group under its subcommittee on medical devices to work toward the development of methods of measurement and defining the limits for hearing aid compatibility and accessibility to wireless telecommunications. The ANSI C63.19 task group is continuing to develop its standard, C63.19–199X, American National Standard for Methods of Measurement for Hearing Aid Compatibility with Wireless Communications Devices. When the standard is completed, the Board may reference it. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

*Question 7:* The Board seeks comment on how to better quantify the ''lowest possible level'' of interference.

Paragraph (e) applies to video or multimedia products. Multimedia products involve more than one media and include, but are not limited to, video programs, narrated slide production, and computer generated presentations.

Paragraph (e)(1) requires any system with a screen larger than 13 inches to be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals. The FCC has standards for televisions 13 inches or larger, but video capabilities are now becoming popular in computers as well. This provision addresses these new video technologies. This provision is consistent with the recommendations of the advisory committee.

Paragraph (e)(2) requires that television tuners, including tuner cards for use in computers, be equipped with the circuitry needed to carry the secondary audio channel. The secondary audio channel is commonly used for audio description. This provision is consistent with the recommendations of the advisory committee.

Paragraphs (e)(3) and (4) require that when an agency develops or procures multimedia productions that are intended to be shown repeatedly to audiences that may include persons who would need the captioning or audio description features, those productions must contain captioning or audio description. Audio description involves the insertion into a multimedia program, such as a video tape, of narrated descriptions of settings and actions that are not otherwise reflected in the dialogue, such as the movement of a person in the scene. Audio description is typically provided through the use of the Secondary Audio Programming (SAP) channel so that it is audible only when that channel is activated through a TV set, computers with a tuner card, or a VCR with SAP capability.

Under these provisions, the requirements to have a videotape or multimedia production captioned or audio described would depend on its intended use. For example, an agency produces, or contracts to have produced, a videotape on government ethics. This videotape is made available for many agencies to purchase and use in training sessions. Since the tape is intended to be shown multiple times and to varied audiences, the composition of which may include people with hearing or vision impairments, it must be captioned and audio described, unless it is an undue burden to do so. On the other hand, a small agency or single office purchases a videotape on some aspect of acoustics which it intends to show to its staff to help understand a technical issue. Since the videotape is not intended to be shown on a repeated basis, and the agency knows that none of its staff have a hearing or vision impairment, the videotape would not need to be captioned or audio described. If however, the video was to be shown to an employee who is deaf, the agency would be required to accommodate that individual by providing an interpreter even though the videotape would not be required to be captioned. Such accommodations would be required under section 501 or 504 of the Rehabilitation Act, not section 508.

*Question 8:* The Board seeks information on the technical feasibility of making various computer generated presentations that comply with these provisions. Based on the proposed rule, computer based narrated slide presentations must be both captioned and audio described if they are shown multiple times and to varied audiences, the composition of which may include people with hearing or vision impairments.

Paragraph (e)(5) provides that viewers must be able to turn captioning or video description features on or off. A person who can hear the audio may find the captioning of conversation intrusive, and people who can see the screen and can hear may find the audio description distracting. For this reason, it is important that an individual have the ability to select or deselect a particular feature.

The advisory committee also recommended that digital television receivers meet the EIA–708–A standard for the transmission of captioning on a digital television signal. The Board has not included this provision since in July 1999, the Federal Communications Commission proposed to amend its rules to include requirements for the display of closed captioned text on digital television receivers. The FCC took this action to ensure that closed captioning services are available in the transition from analog to digital broadcasting. The Board may address this issue in future changes to the standards.

Paragraph (f) applies to information kiosks and information transaction machines. This category of products includes, but is not limited to, automatic teller machines and information kiosks. On November 16, 1999, the Board published a Notice of Proposed Rulemaking to revise and update its accessibility guidelines for buildings and facilities covered by the Americans with Disabilities Act of 1990 (ADA) and the Architectural Barriers Act of 1968 (ABA). 64 FR 62248 (November 16, 1999). Included in that proposed rule are extensive revisions to the requirements for access to automatic teller machines (ATMs) and fare machines. (See sections 707.1;–707.8.3). The proposed revisions to the ADA and ABA guidelines provide more specific guidance on access to such equipment for people with vision impairments. In that proposed rule, the Board requested comment on whether the final rule should cover all types of interactive transaction machines, such as point-of-sale machines and information kiosks, among others, rather than be limited to automatic teller machines and fare vending machines. If the Board decides to broaden the requirements to other types of information transaction machines in the final rule for the ADA and ABA guidelines, the final rule for access to electronic and information technology may not include requirements for information transaction machines since the ADA and ABA rulemaking would apply to the Federal government as well as the private sector.

Paragraph (f)(1) provides that access features must be built into the system rather than requiring users to attach an assistive device to the product. Personal headsets are not considered an assistive device and may be required to use the product. This provision is consistent with the recommendations of the advisory committee.

Paragraph (f)(2) provides that information kiosks and information transaction machines that deliver audio output, including speech, shall provide a mechanism for private listening and user interruptability. A mechanism for private listening means providing either a telephone type handset or a standard jack for headphones. These mechanisms allow users to hear information in private. Allowing the user to interrupt long spoken phrases increases the product's usability and saves time for the user and others who may be waiting to access the product. This provision is consistent with the recommendations of the advisory committee.

Paragraph (f)(3) provides that information kiosks and information transaction machines that deliver voice output, shall provide incremental volume control with output amplification up to a level of at least 65 dB. Where the ambient noise level of the environment is above 45 dB, a volume gain of at least 20 dB above the ambient level shall be user selectable. According to the Occupational Safety and Health Administration, and the American Speech, Language, and Hearing Association, 65 dB is the volume level for normal speech. This provision requires that audio output from a kiosk type product shall have a minimum level of 65 dB. For people with reduced hearing, voice levels must be 20 dB above the surround sound level to be understandable. This means that as long as the noise level in the surrounding environment is below 45 dB, the 65 dB output level would be sufficient. If the product is in an environment with a high noise level, the user must be able to raise the volume to a setting of 20 dB higher than the ambient level. This provision is consistent with the recommendations of the advisory committee.

The advisory committee also recommended standards for remote wireless access to these products. The Board has not included those recommendations since compliant technology is still in development.

### Other Issues

The advisory committee recommended other provisions that the Board did not include in this rule. For example, the committee considered methods for making a personal digital assistant (PDA), such as a ''palmtop,'' accessible for a segment of people with disabilities. The Board has not included such a provision because the technology to make PDAs accessible does not exist at this time.

The committee also recommended that the connection of cables, mounting, and attaching external elements of products (*e.g.*, connecting an external monitor or accessory), require less than 5 pounds of force and that cables be differentiable by touch or keyed for corresponding connections. These provisions are not included since members of the public seeking information from an agency would not be expected to attach or disconnect cables and employees are also covered by sections 501 and 504 of the Rehabilitation Act which require reasonable accommodation to the needs of an employee. Also, connecting and disconnecting cables is not generally an employee task. In the few instances where it is, such as attaching a refreshable Braille display to a laptop, the connections are usually made with standard parallel and serial connectors which are polarized or shaped to prevent incorrect connections. Section 1194.25(b) restricts the use of proprietary connectors.

### Section 1194.25 Requirements for Compatibility With Assistive Technology

Compliant products must be accessible either inherently or by being compatible with add-on assistive technology. The provisions in this section address the requirements for compatibility.

Paragraph (a) provides that all products that act as a transport or conduit for information or communication shall pass all codes, translation protocols, formats, or any other information necessary to provide information or communication in an accessible format. In particular, signal compression technologies shall not remove information needed for access or shall restore it upon decompression.

Some transmissions include codes or tags embedded in ‘‘unused’’ portions of the signal to provide accessibility. For example, closed captioning information is usually included in portions of a video signal not seen by users without decoders. This section prohibits products from stripping out such information or requires the information to be restored at the end point. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (b) requires that, where provided, one of each type of expansion slot, port and connector must comply with publicly available industry standards. This provision applies to hardware products that may require the attachment of assistive technology devices to make them accessible. Examples of publicly available industry standards may include RS–232, Centronics, SCSI interfaces, PCMCIA, or USB.

Paragraph (c) prohibits operating system software from interfering with assistive technology. If an operating system preempts the use of keyboard assignments or the use of specific ports, it can be difficult or impossible to operate the system with assistive technology. This provision requires operating systems to permit the background operation of assistive technology products. This provision is consistent with the recommendations of the advisory committee.

Paragraph (d) requires products with auditory output to provide the auditory signal through an industry standard connector at a standard signal level. Individuals using personal headphones, amplifiers, audio couplers, and other audio processing devices need a place to tap into the audio generated by the product in a standard fashion. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Section 1194.27 Functional Performance Criteria

This section requires that a product’s operation and information retrieval functions be operable through at least one mode which meets each of the following paragraphs.

Paragraph (a) provides that at least one mode of operation and information retrieval that does not require user vision shall be provided, or support for assistive technology used by people who are blind or visually impaired shall be provided. It is not expected that every software program will be self-voicing or have its own built-in screen reader. Providing keyboard access as specified in 1194.23(a) and software that complies with section 1194.23(b) would satisfy this requirement. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (b) provides that at least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 (when corrected with glasses) must be provided in audio and enlarged print output that works together or independently. In the alternative, support for assistive technology used by people who are visually impaired must be provided. Although visual acuity of 20/200 is considered ‘‘legally blind,’’ there are actually millions of Americans with vision below the 20/200 threshold who can still see enough to operate and get output from technology, often with just a little additional boost in contrast or font size. This paragraph requires either the provision of screen enlargement and voice output or, that the product support assistive technology. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (c) provides that at least one mode of operation and information retrieval that does not require user hearing must be provided or, in the alternative, support for assistive technology used by people who are deaf or hard of hearing shall be provided. This requirement is met when a product provides visual redundancy for any audible cues or audio output. If this redundancy cannot be built into a product then the product shall support the use of assistive technology that complies with section 1194.25, Requirements for Compatibility with Assistive Technology. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (d) requires that audio information important for the use of a product, must be provided in an enhanced auditory fashion by allowing for an increase in volume and/or altering the tonal quality or increasing the signal to noise ratio. For example, increasing the output would assist persons with limited hearing to receive information. Audio information that is important for the use of a product includes, but is not limited to, error tones, confirmation beeps and tones, and verbal instructions. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (e) provides that at least one mode of operation and information retrieval which does not require user speech must be provided, or support for assistive technology shall be provided. Most products do not require speech input, however, if speech input is required to operate a product, this paragraph requires that at least one alternative input mode also be provided. For example, an interactive telephone menu that requires the user to say or press ‘‘one’’ would meet this requirement. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (f) provides that at least one mode of operation and information retrieval that does not require fine motor control or simultaneous actions and which is operable with limited reach and strength must be provided. Products that meet the requirements in sections 1194.21(b) and 1194.23(a)(3) would comply with this requirement. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

The advisory committee also recommended provisions that address limited cognitive or memory abilities and limited language and learning disabilities. Although it is important to be cognizant of issues for all people with disabilities, we believe that it is difficult for a manufacturer or procurement official to know if the criteria the committee recommended were met. Also, many of the features required to accommodate other disabilities, can be very useful to people with learning and language related disabilities. For example, features such as voice output and highlighting a focus tracking helps those with reading difficulties.

## *Subpart C—Information, Documentation, and Support*

Section 1194.31 Information, Documentation, and Support

In order for a product or system to be fully accessible, the information about the product and product support services must also be accessible. These issues are addressed in this section.

Paragraph (a) provides that when an agency provides end-user documentation to users of technology, the agency must ensure that the documentation is available upon request in alternate formats. Alternate formats are defined in section 1194.4, Definitions. Except as provided in paragraph (b) below, this provision does not require alternate formats of documentation that is not provided by the agency to other users of technology. This provision is consistent with the recommendations of the advisory committee.

Paragraph (b) requires that agencies supply end-users with information about accessibility or compatibility features that are built into a product, upon request. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

Paragraph (c) provides that help desks and other support services serving an agency must be capable of accommodating the communications needs of persons with disabilities. For example, an agency help desk may need to communicate through a TTY. The help desk or support service must also be familiar with such features as keyboard access and other options important to people with disabilities. This provision is consistent with the Telecommunications Act Accessibility Guidelines and the recommendations of the advisory committee.

The advisory committee also recommended that any training provided by manufacturers, providers or other parties, accommodate the functional capabilities of all participants. The Board has not included this provision since Federal employees already have a right to accessible training under section 504 and other provisions of the Rehabilitation Act.

## Regulatory Process Matters

### *Executive Order 12866: Regulatory Planning and Review and Congressional Review Act*

This proposed rule is an economically significant regulatory action under Executive Order 12866 and has been reviewed by the Office of Management and Budget (OMB). The proposed rule is also a major rule under the Congressional Review Act. The Board has prepared a regulatory assessment for the proposed rule which has been placed in the docket and is available for public inspection. The regulatory assessment is also available on the Board's Internet site (http://www.access-board.gov/rules/508nprm.htm).

Section 508 covers the development, procurement, maintenance or use of electronic and information technology by Federal agencies. Exemptions are provided by statute for national security systems and for instances where compliance would impose an undue burden on an agency. The proposed rule improves the accessibility of electronic and information technology used by the Federal government and will affect Federal employees with disabilities, as well as members of the public with disabilities who seek to use Federal electronic and information technologies to access information. The proposed rule is based largely on the recommendations of the Electronic and Information Technology Access Advisory Committee.

The standards in the proposed rule will be incorporated into the Federal Acquisition Regulation (FAR). Failure of a Federal agency to comply with the standards may result in a complaint under the agency's existing complaint procedures under section 504 of the Rehabilitation Act or a civil action seeking to enforce compliance with the standards.

### Estimated Baseline of Federal Spending for Electronic and Information Technology

According to OMB projections, Federal government expenditures for information technology products will be $38 billion in fiscal year 2000. The defense agencies appear to have the highest information technology budgets, while civilian agency budgets are expected to increase rapidly. It was not possible however, to disaggregate this data such that it was useful for purposes of a regulatory assessment. Instead, the regulatory assessment uses annual sales data collected from the General Services Administration (GSA) as a proxy for the actual number of products in each applicable technology category. Using the GSA data, the regulatory assessment estimates that the Federal government spends approximately $12.4 billion annually on electronic and information technology products covered by the proposed rule. This estimate likely understates the actual spending by the Federal government because it is limited to the GSA data. Agencies are not required to make purchases through the GSA supply service, thus many items are purchased directly from suppliers. As a result, the government costs for software and compatible hardware products may actually be higher than estimates would indicate.

The regulatory assessment also examines historical budgetary obligations for information technology tracked by OMB until 1998. Two scenarios were examined to develop an upper and lower bound to represent the proportion expected to be potentially affected by the proposed rule. During a five year period from fiscal year 1994 through fiscal year 1998, the average proportion of the total information technology obligations potentially covered by the proposed rule ranged between 25 percent and 50 percent. The $12.4 billion GSA estimate falls within this range, representing 33 percent of the total fiscal year 1999 information technology obligations of $38 billion. One limitation of these ranges is that they are based on gross classifications of information technology obligations and do not provide the level of disaggregation necessary to parallel the GSA data assessment. As a result, the two scenarios likely include expenditures on products and services that would not be effected by the proposed rule to a higher degree than the data obtained from GSA.

The degree to which the potential understatement of baseline spending leads to an understatement of the cost of the proposed rule is unclear. Some of the components of the estimated cost of the proposed rule rely heavily on the level of Federal spending while others are independent of this number.

*Question 9:* The Board seeks information, other than that collected from GSA, which would provide additional product specific data to further assess the cost impact of this rule. The data should cover either the entire, or at least a representative majority, of Federal government acquisitions of electronic and information technology; or capture non-GSA procurements.

### Estimated Cost of Proposed Rule

The regulatory assessment includes both direct and opportunity costs associated with the proposed rule. Major sources of cost include:

- Costs of modifying electronic and information technology to meet the substantive requirements of the standards;
- Training of staff, both Federal and manufacturers, to market, support, and use technologies modified in response to the standards; and
- Translation of documentation and instructions into alternate formats.

The direct costs that were quantified are shown in Table 1. The total quantified costs to society range from $177 million to $1,068 million annually. The Federal proportion of these costs is estimated to range between $85 million and $691 million. The ability of manufacturers, especially software manufacturers, to distribute these costs over the general consumer population will determine the actual proportion shared by the Federal government.

Assuming that the addition of accessibility features add value to the products outside the Federal government, it is expected that the costs will be distributed across society thereby setting a lower bound cost to the Federal government of $85 million. If manufacturers do not distribute the costs across society, the upper bound of the Federal cost will increase to an estimated $1,068 million. These costs must be placed in appropriate context by comparing them with the total Federal expenditures for information technology. By comparison, the lower and upper bound of the incremental costs represent a range of 0.23 percent to 2.8 percent of the $38 billion spent by the Federal government on information technology in fiscal year 1999. Although the regulatory assessment does not analyze the timing of expenditures or reductions in costs over time, it is expected that the costs will decrease over time as a proportion of total electronic and information technology spending.

TABLE 1

| Electronic and information technology | Lower bound cost estimates (millions) | Upper bound cost estimates (millions) |
|---|---|---|
| General Office Software | $110 | $456 |
| Mission Specific Software | 10 | 52 |
| Compatible Hardware Products | | 337 |
| Document Management Products | 56 | 222 |
| Microphotographic Products | 0.1 | 0.4 |
| Other Miscellaneous Products | 0.2 | 1 |
| Total Social Cost | 177 | 1,068 |
| Estimated Federal Proportion | 85 | [1]691 |

[1] As noted above, if manufacturers do not distribute the costs across society, the upper bound of the Federal cost will increase to an estimated $1,068 million.

Accessible alternatives are available to satisfy the requirements of the proposed rule for many types of electronic and information technologies, particularly computers and software products. Some electronic and information technology products will require modifications to meet the requirements of the proposed standards.

For many types of electronic and information technology, the proposed rule focuses on compatibility with existing and future assistive devices, such as screen readers. The proposed rule does not require that assistive technologies be provided universally. Provision of assistive technologies is still governed by the reasonable accommodation requirements contained in sections 501 and 504 of the Rehabilitation Act. Section 508 does not require that assistive devices be purchased, but it does require that covered electronic and information technology be capable of having such devices added at some later time as necessary.

Software products represent the largest part of the estimated costs. The regulatory assessment assumes that Federal software expenditures can be divided into two major subcategories: general office applications and mission-specific applications. Internet applications are assumed to be represented within each of these subcategories. General office applications include operating systems, wordprocessors, and spreadsheets, and are assumed to represent 80 percent of the total software category. The remaining 20 percent covers mission-specific or proprietary applications that have limited distribution outside the Federal government. Within each subcategory, the estimated costs of the proposed rule are distributed according to the level or degree of accessibility already being achieved in the private sector.

The general office application subcategory is broken into three groups based on discussions with several industry experts. The first 30 percent is expected to require very little modification to satisfy the proposed standards and therefore no incremental cost is associated with this group. The middle 40 percent is expected to require minor to medium alterations to satisfy the proposed rule. The cost of modifying a particular general office application in this category is estimated to be in the range of 0.4 percent to 1 percent based on discussions with several manufacturers. This assumption is based on the ratio of employees dedicated to accessibility issues. The methodology uses employee classification as a proxy for cost or expense of accessibility research and development, labor, and design that are all factored into the final product cost. The remaining 30 percent is expected to require significant modifications to meet the requirements of the proposed rule, which is estimated to cost in the range of 1 percent to 5 percent based on discussion with industry experts.

The regulatory assessment assumes that the remaining 20 percent of the software products purchased by the Federal government represent proprietary or mission-specific software with limited distribution outside the government. These products will require significant modification to satisfy the proposed rule. Based on discussions with industry experts, the cost increase associated with achieving the level of accessibility required by the proposed rule is estimated to range from 1 percent to 5 percent.

*Question 10:* The Board requests comments on the assumptions applied to determine the cost associated with software products. The Board also seeks comment on alternative methods or data sources for evaluating the Federal government's expenditure on software products.

### Estimated Benefits of Proposed Rule

The benefits associated with the proposed rule results from increased access to electronic and information technology for Federal employees with disabilities and members of the public seeking Federal information provided using electronic and information technology. This increased access reduces barriers to employment in the Federal government for persons with disabilities, reduces the probability that Federal employees with disabilities will be underemployed, and increases the productivity of Federal work teams. The proposed standards may also have benefits for people outside the Federal workforce, both with and without disabilities, as a result of spillover of technology from the Federal government to the rest of society.

Two methods are presented in the regulatory assessment for evaluating the quantifiable benefits of the proposed rule. The first is a wage gap analysis that attempts to measure the difference in wages between the general Federal workforce and Federal workers with disabilities (*i.e.,* targeted and reportable). While this analysis is limited to white collar Federal workers due to data constraints, the potential change in productivity is measured by the difference between the weighted average salary for all white collar Federal employees and the average within the two disability classes. This assumes that an increase in accessibility will help diminish this wage gap by increasing worker productivity.

The alternative is a team based approach for measuring the productivity of Federal workers. This approach is based on the assumption that a Federal workers wage rate reflects their productivity and the scarcity of their skills in the labor market. However this may not apply to Federal wage rates, thus the average productivity of a Federal team is assumed to be equivalent to the average Federal wage rate. Based on this average rate, it is assumed that the proposed rule will produce an increase in productivity ranging between 5 percent and 10 percent.

Since no data have been identified to support the increase in productivity in the team based approach, the wage gap analysis is used to represent the benefits generated by the proposed rule shown in Table 2. Keeping in mind certain data limitations with this analysis, the benefits derived from the wage gap method do not account for benefits that may be accrued by the general public or other Federal workers due to spillover effects of increased accessibility resulting from the proposed standards.

TABLE 2

| Productivity increase | Aggregate benefits range (millions) |
|---|---|
| Lower Bound | |
| Upper Bound | $466 |

Not all government policies are based on maximizing economic efficiency. Some policies are based on furthering the rights of certain classes of individuals to achieve more equitable results, regardless of the effect on economic efficiency. Accessibility to electronic information and technology is an essential component of civil rights for persons with disabilities. The proposed rule will ensure that Federal employees with disabilities will have access to electronic and information technology used by the Federal government that is comparable to that of Federal employees without disabilities; and that members of the public with disabilities will have comparable access to information and services provided to members of the public without disabilities through the use of Federal electronic and information technology.

Based on Bureau of Census statistics from 1994,[14] 20.6 percent or 54 million persons in the United States have some level of disability. By increasing the accessibility of electronic and information technology used by the Federal government, the proposed rule may also improve future employment opportunities in the Federal government for persons with disabilities currently employed by the Federal government, and for persons that are working in the private sector or are classified as not being active in the labor force. Increasing the accessibility of electronic and information technology increases the productivity and mobility of the disabled sector of the labor pool that, under existing conditions, may face barriers to their employment and advancement within the Federal workforce and in the private sector.

*Question 11:* The Board requests comment on the sufficiency of the benefits assessment and seeks recommendations for alternative methods of evaluating the benefits generated by the proposed rule for persons with disabilities, including the public as a whole.

### *Executive Order 13132: Federalism*

By its terms, this proposed rule focuses on the development, procurement, maintenance or use by Federal agencies of electronic and information technology. As such, the Board believes that it does not have federalism implications within the meaning of Executive Order 13132. The Board is aware, however, that the Department of Education interprets the Assistive Technology Act (the ''AT Act''), 29 U.S.C. 3001, to require that States receiving assistance under the AT State Grants program to comply with section 508, including these standards. The Department of Education, the agency responsible for administering the AT Act, has advised the Board that it plans to issue guidance to explain specifically how these proposed standards would apply to the States for purposes of the AT Act. In this regard, the Department of Education plans to consult with State and local governments in a manner consistent with the requirements of Executive Order 13132, and to urge them to comment to the Access Board on the content of the proposed rule during the public comment period. The Board recommends that any other Federal agency considering whether (or how) to apply these standards to non-Federal entities, or any agency required to apply these standards to non-Federal entities by provision of law, should similarly conduct an appropriate consultation process with all affected stakeholders. The Board welcomes comment on any federalism implications associated with this proposed rule.

### *Unfunded Mandates Reform Act*

The Unfunded Mandates Reform Act does not apply to proposed or final rules that enforce constitutional rights of individuals or enforce any statutory rights that prohibit discrimination on the basis of race, color, sex, national origin, age, handicap, or disability. Since the proposed rule is issued under the authority of section 508, part of title V of the Rehabilitation Act of 1973 which establishes civil rights protections for individuals with disabilities, an assessment of the rule's effects on State, local, and tribal governments, and the private sector is not required by the Unfunded Mandates Reform Act.

### List of Subjects in 36 CFR Part 1194

Civil rights, Communications equipment, Computer technology, Electronic products, Government employees, Government procurement, Individuals with disabilities, Reporting and recordkeeping requirements, Telecommunications.

**Thurman M. Davis, Sr.,**
*Chair, Architectural and Transportation Barriers Compliance Board.*

For the reasons set forth in the preamble, the Board proposes to add part 1194 to Chapter XI of title 36 of the Code of Federal Regulations to read as follows:

## PART 1194—ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY STANDARDS

### Subpart A—General

### Subpart B—Accessibility Standards

### Subpart C—Information, Documentation, and Support

### Figures to Part 1194

**Authority:** 29 U.S.C. 794d.

## Subpart A—General

### § 1194.1 Purpose.

The purpose of this part is to implement section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d). Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal

[14] U.S. Department of Commerce, Economics and Statistics Administration, ''Americans with Disabilities: 1994–95'' (P70–61), August 1997.

employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

### § 1194.2 Application.

(a) When developing, procuring, maintaining, or using electronic and information technology, each agency shall comply with the requirements of this part, unless an undue burden would be imposed on the agency.

(1) When compliance with the requirements of this part imposes an undue burden, agencies shall provide individuals with disabilities with the information and data involved by an alternative means of access that allows the individual to use the information and data.

(2) When procuring a product, if an agency determines that compliance with any requirement of this part imposes an undue burden, the documentation by the agency supporting the procurement shall explain why, and to what extent, compliance with each such requirement creates an undue burden.

(b) Except as provided by § 1194.3(b), this part applies to electronic and information technology developed, procured, maintained, or used by agencies directly or used by a contractor under a contract with an agency which requires the use of such product, or requires the use, to a significant extent, of such product in the performance of a service or the furnishing of a product.

(c) This part applies to products procured by agencies when such products are:

(1) Available in the commercial marketplace;

(2) Not yet available in the commercial marketplace, but through advances in technology or performance will be available in time to satisfy the delivery requirements under a Government solicitation; or

(3) Developed in response to a Government solicitation.

(d) Products required to be accessible shall comply with all applicable provisions of this part. Section 1194.21 provides requirements that apply generally to all products. Section 1194.23 provides requirements for specific components of products and shall be applied to each component. Products may have more than one component. Section 1194.25 provides requirements for compatibility of products with assistive technology commonly used by individuals with disabilities. Section 1194.27 provides functional performance criteria for overall product evaluation and for technologies or components for which there is no specific requirement under other sections. Section 1194.31 provides requirements for information, documentation, and support.

### § 1194.3 General exceptions.

(a) This part does not apply to any telecommunications or information system operated by agencies, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or systems which are critical to the direct fulfillment of military or intelligence missions. Systems which are critical to the direct fulfillment of military or intelligence missions do not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(b) This part does not apply to electronic and information technology that is acquired by a contractor incidental to a contract.

(c) Except as required to comply with the standards in this part, this part does not require the installation of specific accessibility-related software or the attachment of an assistive technology device at a workstation of a Federal employee who is not an individual with a disability.

(d) When agencies provide access to the public to information or data through electronic and information technology, agencies are not required to make equipment owned by the agency available for access and use by individuals with disabilities at a location other than that where the electronic and information technology is provided to the public, or to purchase equipment for access and use by individuals with disabilities at a location other than that where the electronic and information technology is provided to the public.

(e) This part shall not be construed to require a fundamental alteration in the nature of a product or its components.

### § 1194.4 Definitions.

The following definitions apply to this part:

*Accessible.* Electronic and information technology which complies with the requirements of this part.

*Agency.* Any Federal department or agency, including the United States Postal Service.

*Alternate formats.* Alternate formats usable by people with disabilities may include, but are not limited to, Braille, ASCII text, large print, recorded audio, and accessible internet programming or coding languages.

*Alternate modes.* Different means of providing information, including product documentation, to people with disabilities. Alternate modes may include, but are not limited to, voice, fax, relay service, TTY, Internet posting, captioning, text-to-speech synthesis, and audio description.

*Assistive technology.* Any item, piece of equipment, or system, whether acquired commercially, modified, or customized, that is commonly used to increase, maintain, or improve functional capabilities of individuals with disabilities.

*Electronic and information technology.* Includes information technology and any equipment or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information. The term electronic and information technology includes, but is not limited to, telecommunications products (such as telephones), information kiosks and transaction machines, World Wide Web sites, multimedia, and office equipment such as copiers and fax machines. The term does not include any equipment that contains imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

*Information technology.* Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term *information technology* includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

*Operable controls.* A component of a product that requires physical contact for normal operation. Operable controls include, but are not limited to, mechanically operated controls, paper trays, card slots, keyboards, or keypads.

*Product.* Electronic and information technology.

*Telecommunications.* The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

*TTY.* An abbreviation for teletypewriter. Machinery or equipment that employs interactive text based communications through the transmission of coded signals across the telephone network. TTYs may include, for example, devices known as TDDs (telecommunication display devices or telecommunication devices for deaf persons) or computers with special modems. TTYs are also called text telephones.

*Undue burden.* Undue burden means significant difficulty or expense. In determining whether an action would result in an undue burden, an agency shall consider all agency resources available to the agency or components for which the product is being developed, procured, maintained, or used.

### § 1194.5 Equivalent facilitation.

Nothing in this part is intended to prevent the use of designs or technologies as alternatives to those prescribed in this part provided they result in substantially equivalent or greater access to and use of a product for people with disabilities.

## Subpart B—Accessibility Standards

### § 1194.21 General requirements.

(a) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

(b) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following:

(1) The position of any operable control shall be determined with respect to a vertical plane, which is 48 inches in length, centered on the operable control, and at the maximum protrusion of the product within the 48 inch length (see Fig. 1 of this part).

(2) Where any operable control is 10 inches or less behind the reference plane, the height shall be 54 inches maximum and 15 inches minimum above the floor.

(3) Where any operable control is more than 10 inches and not more than 24 inches behind the reference plane, the height shall be 46 inches maximum and 15 inches minimum above the floor.

(4) Operable controls shall not be more than 24 inches behind the reference plane (see Fig. 2 of this part).

(c) When flashing or blinking text, objects, or other elements are displayed, the flash rate shall not exceed two Hertz.

(d) If a timed response is required, at least one mode which does not require users to respond within a timed interval or allows users to adjust the timing and repetition of those intervals to at least 5 times the default setting, shall be provided.

(e) Where biometric forms of user identification or activation are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.

(f) Where touchscreens or touch-operated controls are used, such controls shall be operable without requiring body contact or close human body proximity, or all of the operations and functions that are available through such controls shall be made available through an alternate mode that does not require body contact or close human body proximity.

### § 1194.23 Component specific requirements.

(a) *Mechanically operated controls, keyboards or keypads.* (1) Controls and keys shall be tactilely discernible without activating the controls or keys.

(2) The status of all locking or toggle controls or keys shall be visually discernible, and discernible either through touch or sound.

(3) Controls shall be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls shall be 5 lbs. (22.2 N) maximum.

(4) All actions available or required by the product shall be available from the keyboard or keypad.

(5) If keyboard repeat is supported, the keyboard delay before repeat shall be adjustable to at least 2 seconds. Key repeat rate shall be adjustable to 2 seconds per character.

(b) *Non-embedded software applications and operating systems.*

(1) Logical navigation among interface elements shall be provided by use of keystrokes.

(2) Software shall not interfere with existing features of other products or operating systems that affect the usability for people with disabilities.

(3) A well-defined on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that assistive technology can track focus and focus changes.

(4) Sufficient information about a user interface element including the identity, operation and state of the element shall be available to assistive technology.

(5) Where an image represents an interface element or the state of an interface element, there must be a way for assistive technology to associate meaningful text with the image.

(6) The use of images shall be consistent throughout an application.

(7) Text shall be provided through an application programming interface supporting interaction with assistive technology or use system text writing tools. The minimum information that shall be available to assistive technology is text content, text input caret location, and text attributes.

(8) A minimum of 8 foreground and 8 background color selections capable of producing a variety of contrast levels shall be provided.

(9) An option shall be provided to ignore individual application display attributes so system-wide settings will be maintained.

(10) Electronic forms shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form including all directions and cues. Inaccessible electronic forms may be used, if an alternative accessible electronic form with equivalent information, field elements, and functionality is also provided.

(11) If animated or moving text is provided it shall also be displayable in at least one static presentation mode at the option of the user.

(c) *Web-based information or applications.*

(1) A text equivalent for every non-text element shall be provided via ''alt'' (alternative text attribute), ''longdesc'' (long description tag), or in element content.

(2) Web pages shall be designed so that all information required for navigation or meaning is not dependent on the ability to identify specific colors.

(3) Changes in the natural language (*e.g.,* English to French) of a document's text and any text equivalents shall be clearly identified.

(4) Documents shall be organized so they are readable without requiring an associated style sheet.

(5) Web pages shall update equivalents for dynamic content whenever the dynamic content changes.

(6) Redundant text links shall be provided for each active region of a server-side image map.

(7) Client-side image maps shall be used whenever possible in place of server-side image maps.

(8) Data tables shall provide identification of row and column headers.

(9) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.

(10) Frames shall be titled with text that facilitates frame identification and navigation.

(11) Pages shall be usable when scripts, applets, or other programmatic objects are turned off or are not supported, or shall provide equivalent information on an alternative accessible page.

(12) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.

(13) An appropriate method shall be used to facilitate the easy tracking of page content that provides users of assistive technology the option to skip repetitive navigation links.

(d) *Telecommunications functions.* (1) Telecommunications products which provide a function allowing voice communication and which do not themselves provide a TTY functionality shall provide a standard non-acoustic connection point for TTYs. It shall also be possible for the user to easily turn any microphone on and off to allow the user to intermix speech with TTY use.

(2) Telecommunications products which include voice communication functionality shall support use of all cross-manufacturer non-proprietary standard signals used by TTYs.

(3) Voice mail, auto-attendant, and interactive voice response telecommunications systems shall be usable by TTY users with their TTYs.

(4) Voice mail, messaging, auto-attendant, and interactive voice response telecommunications systems shall provide at least one mode which does not require users to respond within a timed interval or allows users to adjust the timing and repetition of those intervals to a minimum of 5 times the default.

(5) Where provided, caller identification and similar telecommunications functions shall also be available for users of TTYs, telecommunications relay services, and for users who cannot see displays.

(6) For transmitted voice signals, telecommunications products shall provide a gain adjustable up to a minimum of 20 dB. For incremental volume control, at least one intermediate step of 12 dB of gain shall be provided.

(7) If the telecommunications product allows a user to adjust the receive volume, a function shall be provided to automatically reset the volume to the default level after every use but not before.

(8) Where a telecommunications product delivers output by an audio transducer, which is normally held up to the ear, a means for effective magnetic wireless coupling to hearing technologies shall be provided.

(9) Interference to hearing technologies (including hearing aids, cochlear implants, and assistive listening devices) shall be reduced to the lowest possible level that allows a user of hearing technologies to utilize the telecommunications product.

(e) *Video or multimedia products.* (1) All television displays 13 inches and larger, and computer equipment that includes television receiver circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals.

(2) Television tuners, including tuner cards for use in computers, shall be equipped with secondary audio program playback circuitry.

(3) All video and multimedia productions, regardless of format, that contain speech or other audio necessary for the comprehension of the content, shall be open or closed captioned if the production is procured or developed for repeated showings to audiences that may include people with hearing impairments.

(4) All video and multimedia productions, regardless of format, that contain visual information necessary for the comprehension of the content, shall be audio described if the production is procured or developed for repeated showings to audiences that may include people with visual impairments.

(5) Display or presentation of alternate text presentation or audio descriptions shall be user-selectable unless permanent.

(f) *Information kiosks and transaction machines.* (1) Information kiosks and transaction machines shall be usable by people with disabilities without requiring an end-user to attach assistive technology to the information kiosk or transaction machine.

(2) Where information kiosks and transaction machines deliver audio output, including speech, a mechanism shall be provided for private listening and user interruptability.

(3) Where information kiosks and transaction machines deliver voice output, incremental volume control shall be provided with output amplification up to a level of at least 65 dB. Where the ambient noise level of the environment is above 45 dB, a volume gain of at least 20 dB above the ambient level shall be user selectable.

### § 1194.25 Requirements for compatibility with assistive technology.

(a) All products that act as a transport or conduit for information or communication shall pass through cross-manufacturer, non-proprietary, industry-standard codes, translation protocols, formats or other information necessary to provide the information or communication in a usable format. Technologies which use encoding, signal compression, format transformation, or similar techniques shall not remove information needed for access or shall restore it upon delivery.

(b) Where provided, at least one of each type of expansion slots, ports and connectors shall comply with publicly available industry standards.

(c) Operating system software shall not interfere with assistive technology.

(d) Products providing auditory output shall provide the auditory signal at a standard signal level through an industry standard connector.

### § 1194.27 Functional performance criteria.

(a) At least one mode of operation and information retrieval that does not require user vision shall be provided, or support for assistive technology used by people who are blind or visually impaired shall be provided.

(b) At least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 shall be provided in audio and enlarged print output working together or independently, or support for assistive technology used by people who are visually impaired shall be provided.

(c) At least one mode of operation and information retrieval that does not require user hearing shall be provided, or support for assistive technology used by people who are deaf or hard of hearing shall be provided.

(d) Where audio information is important for the use of a product, at least one mode of operation and information retrieval shall be provided in an enhanced auditory fashion.

(e) At least one mode of operation and information retrieval that does not require user speech shall be provided, or support for assistive technology shall be provided.

(f) At least one mode of operation and information retrieval that does not require fine motor control or simultaneous actions and that is operable with limited reach and strength shall be provided.

## Subpart C—Information, Documentation, and Support

### § 1194.31 Information, documentation, and support.

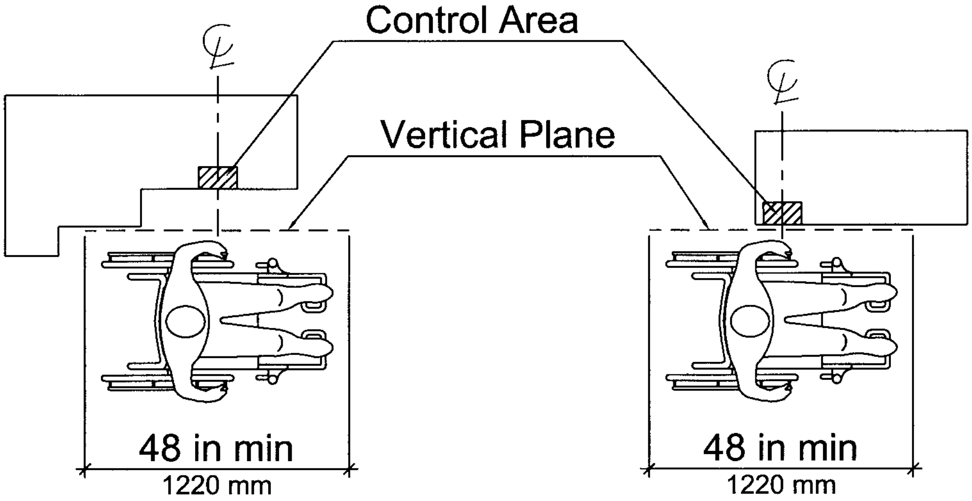
(a) Agencies shall ensure that any product support documentation provided by the agency to end-users, is available in alternate formats upon request, at no additional charge.

(b) Agencies shall ensure that end-users have access to a description of the accessibility and compatibility features of products provided by the agency in alternate formats or alternate modes upon request, at no additional charge.

(c) Agencies shall ensure that support services for products provided by the agency, will accommodate the communication needs of end-users with disabilities.

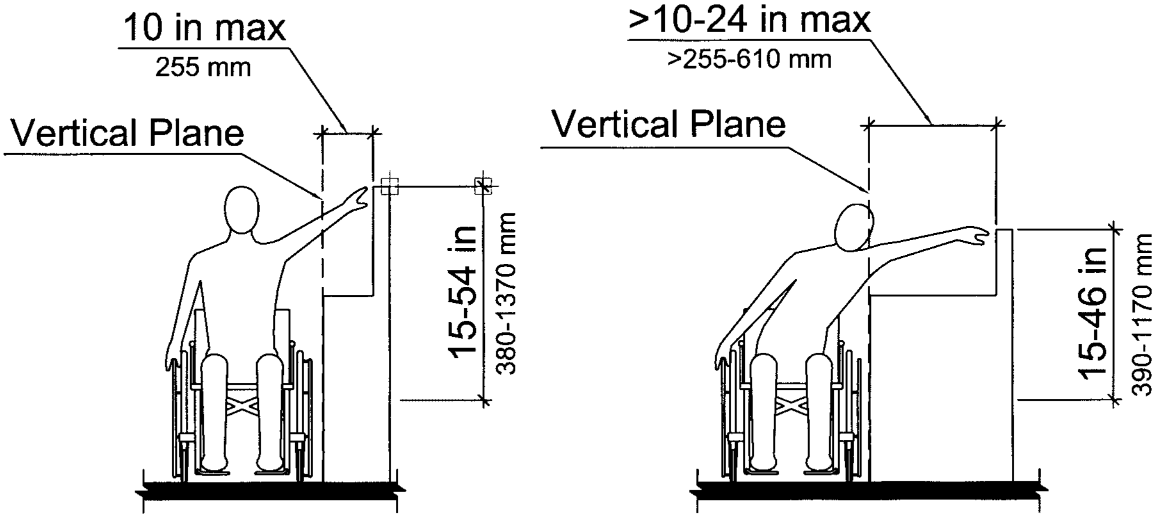
BILLING CODE 8150–01–P

**Figures to Part 1194**



Vertical Plane Relative to the Operable Control

## Figure 1



Height of Operable Control Relative to the Vertical Plane

## Figure 2

[FR Doc. 00–7719 Filed 3–30–00; 8:45 am]

BILLING CODE 8150–01–C